



Brussels, 25 July 2025  
(OR. en)

11953/25  
ADD 5

GAF 19  
FIN 922

## COVER NOTE

---

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	25 July 2025
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union

---

No. Cion doc.:	SWD(2025) 199 final
Subject:	Commission staff working document: Follow-up by Member States to the recommendations of the PIF Report 2023 accompanying the document "Report from the Commission to the Council and the European Parliament: 36th Annual Report on the protection of the European Union's financial interests and the fight against fraud - 2024"

---

Delegations will find attached document SWD(2025) 199 final.

---

Encl.: SWD(2025) 199 final



EUROPEAN  
COMMISSION

Brussels, 25.7.2025  
SWD(2025) 199 final

## **COMMISSION STAFF WORKING DOCUMENT**

**Follow-up by Member States to the recommendations of the PIF Report 2023**

*Accompanying the document*

### **REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT**

**36th Annual Report on the protection of the European Union's financial interests and  
the fight against fraud - 2024**

{COM(2025) 426 final} - {SWD(2025) 196 final} - {SWD(2025) 197 final} -  
{SWD(2025) 198 final} - {SWD(2025) 228 final} - {SWD(2025) 229 final} -  
{SWD(2025) 230 final}

<b>Introduction.....</b>	<b>7</b>
<b>1. Overview of Member States' replies to the questionnaire .....</b>	<b>8</b>
<b>1.1. Recommendation 1: Improving the reporting and follow-up of suspected fraud.....</b>	<b>8</b>
1.1.1 Confidence in reporting systems .....	8
1.1.2 Issues with information flow .....	9
1.1.3 Best practices mentioned by Member States .....	10
<b>1.2. Recommendation 2: Accelerating the digitalisation of the fight against fraud .....</b>	<b>10</b>
1.2.1 Current status and challenges in digitalisation.....	11
1.2.2. Approaches to achieve interoperability mentioned by Member States .....	15
1.2.3. State-of-play and utilisation of ARACHNE .....	16
1.2.4. Advantages vs difficulties with the use of ARACHNE .....	18
<b>1.3. Recommendation 3: Reinforcing anti-fraud governance in the Member States.....</b>	<b>19</b>
1.3.1. State-of-play in national anti-fraud governance structures .....	19
1.3.2. Best practices in anti-fraud governance .....	20
<b>2. Responses from the Member States .....</b>	<b>21</b>
Q.1.1 Have you reviewed the effectiveness of your reporting in the Irregularity Management System (IMS) in 2024? .....	21
Q.1.2 If “YES” to Q.1.1, What were the main findings of your evaluation? .....	21
Q.1.3 How would you evaluate your level of maturity of your current reporting process for reporting irregularities and, in particular, fraud? .....	24
Following Q1.3, please specify "Other". .....	25
Q.1.4 Can you provide examples of well-established reporting systems or practices that have been effective in capturing and reporting suspected fraud cases and irregularities? .....	25
Q.1.5 Have you identified in 2024 new weaknesses in your reporting practices that could hinder the timely and exhaustive reporting in IMS, in particular of suspected fraud cases? .....	33
Q.1.6 If “YES” to Q.1.5, in which of the following areas did you encounter new difficulties? .....	33
Following Q1.6, please specify "Other". .....	33
Q.1.7 Have you made significant improvements to the quality of your reporting on suspected fraud cases and irregularities in 2024? .....	34
Q.1.8 What are the main steps you have taken to improve the reporting of irregularities? .....	34
Following Q1.8, please specify "Other". .....	35
Q.1.9 If “NO, not yet” or “NO” to Q.1.7, what are the main reasons preventing you from further improving the quality of reporting in 2024? .....	36
Following Q1.9, please specify "Other". .....	36
Q.1.10 In 2024, have you encountered any difficulties in providing timely updates about the follow-up to irregularities, and in particular, fraudulent irregularities? .....	36
Q.1.11 In which areas did you encounter more difficulties when updating already reported fraudulent irregularities? .....	37

Following Q1.11, please specify "Other".	37
Q.1.12 Regarding previous question, please provide additional explanation about the difficulties encountered.	38
Q.1.13 Has the information flow between judicial and reporting authorities improved in 2024?	40
Q.1.14 If “YES, fully” and “YES, partly” to Q.1.13, what steps have been taken in 2024 to improve the exchange of information between judicial and reporting authorities?	40
Following Q1.14, please specify "Other".	41
Q.1.15 Can you provide a short description of the organisational structure and procedures for exchanging information between judicial authorities and reporting authorities in your Member State?	42
Q.1.16 What methods are used for exchanging information between judicial and reporting authorities?	49
Following Q1.16, please specify "Other".	50
Q.1.17 Do you see possible improvement in the exchange of information between judicial and reporting authorities? If yes, which ones? How can OLAF / the Commission support this?	53
Q.1.18 Please feel free to share any additional thoughts or experiences you have regarding the topics discussed in this section.	56
Q.2.1. Have you ensured that the digitalisation of the fight against fraud is part of your NAFS (National anti-fraud strategy)?	59
Following Q.2.1, please specify "Digitalisation of the fight against fraud is part of another strategy / assessment / policy".	59
Q.2.2. If “YES” to Q.2.1, please describe how it has been implemented.	61
Q.2.3. If “NO” to Q.2.1, please explain why the digitalisation of the fight against fraud is not part of your NAFS nor of any other strategic approach.	70
Q.2.4 What are the main gaps you have identified in the digitalisation of your anti-fraud efforts?	70
Q.2.5 What steps have you undertaken to address gaps in the digitalisation of your anti-fraud efforts?	71
Following Q.2.5, please specify "Other".	72
Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud? Inventory of existing tools: conduct a thorough inventory of existing digital tools and technologies used in the fight against fraud.	73
Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud? Benchmarking on new trends: conduct benchmarking research on new trends and technologies used in the fight against fraud.	73
Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Evaluation and updates of existing IT tools.	74
Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Development/deployment of new, dedicated IT tools.	74
Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Improve interoperability between systems already in use to enhance data sharing.	74
Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Dedicated allocated staff / resources / taskforce.	75
Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Trainings of the staff.	75

Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Risk analysis assessment.....	75
Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Other (please specify in the next question).....	76
Q.2.7 Following Q.2.6, please specify any other actions you have taken, or you have planned on taking to keep up with evolving new technologies used to commit fraud.....	76
Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Inventory of existing tools: conduct a thorough inventory of existing digital tools and technologies used in the fight against fraud.....	78
Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Benchmarking on new trends: conduct benchmarking research on new trends and technologies used in the fight against fraud .....	79
Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Evaluation and updates of existing IT tools.....	79
Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Development/deployment of new, dedicated IT tools.....	80
Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Improve interoperability between systems already in use to enhance data sharing .....	80
Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Dedicated allocated staff / resources / taskforce .....	80
Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Trainings of the staff.....	81
Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Risk analysis assessment.....	81
Polar plot of the Average Level of Importance Assigned to Anti-Fraud Action.....	82
Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Use of AI (Artificial Intelligence) .....	82
Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Data Analysis tools (external).....	83
Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Automated data analysis tools (integrated).....	83
Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Predictive analytics.....	83
Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Database integration .....	84
Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Fraud case management system .....	84
Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Cross-agency data sharing.....	84
Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Cybersecurity measures .....	85
Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Automation of information exchange .....	85

Spiderplot of Average Stage of Implementation of Digital Tools and Technologies Across All Member States.....	86
Q.2.10 Following Q.2.9, please specify any other digital tools or technologies you are using, or you are planning to use. ....	86
Q.2.11 Are your data analysis tools integrated directly into your databases, or do you deploy external systems for data analysis?.....	90
Following Q.2.11, please specify "Other". ....	90
Q.2.12 Does your data management system facilitate interoperability?.....	91
Q.2.13 If YES to Q.2.12, could you describe how interoperability is achieved between your data analysis tools and databases? .....	91
Q.2.14 Does your digitalisation strategy prioritize the standardized use of digital tools and technologies across local levels and different administrations so that all authorities involved in the anti-fraud strategy can access it? .....	94
Following Q.2.14, please specify "Other". ....	94
Q.2.15 How do you evaluate the successful implementation of the digital tools at different administrative levels? .....	95
Following Q.2.15, please specify "Other". ....	95
Q.2.16 To what extent have digital tools been spread and adopted across different administrative levels? ...	96
Following Q.2.16, please specify "Limited dissemination to specific regions/localities only ". ....	96
Following Q.2.16, please specify "Other". ....	96
Q.2.17 What are the key challenges you face in accelerating the digitalisation of your fight against fraud? .	97
Following Q.2.16, please specify "Other". ....	98
Q.2.18 Has your Member State conducted evaluations to assess the interoperability of national systems with Arachne? .....	98
Q.2.19 If “YES” to Q.18, Please provide key findings or the stage of completion concerning system interoperability.....	99
Q.2.20 What steps have you undertaken to ensure your systems are prepared to feed data into Arachne for the upcoming multiannual financial framework? Please refer to the indicative milestones from figure 1 and select the ones you have reached. ....	100
Following Q.2.20, please specify "Other ". ....	101
Q.2.21 Currently, what are the factors preventing you from being able to feed the data into Arachne? .....	102
Q.2.22 What type of support would facilitate your successful integration of data into Arachne by the required deadline? .....	103
Following Q.2.21, please specify "Other ". ....	103
Q.2.22 What type of support would facilitate your successful integration of data into Arachne by the required deadline? .....	104
Following Q.2.22, please specify "Other ". ....	104
Q.2.23 As part of your anti-fraud strategies, are you considering the use of Arachne? .....	105
Q.2.24 If “Already in use” or “planning to use” to Q.2.21, please elaborate on your (planned) use of the tool. If “No plans to use”, please provide a brief explanation for not planning to use Arachne. ....	105
Q.2.25 Has your Member State implemented ARACHNE? .....	109

Q.2.26 If “YES” to Q.2.25, please specify the entities or individuals that have access to the Member State's data within the Arachne system. ....	109
Following Q.2.26, please specify "Other ". ....	109
Q.2.27 If “YES” to Q.2.25, what is the tool used for? .....	110
Q.2.28 If “YES” to Q.2.25, since implementing it, how has it impacted the efficiency and effectiveness of your anti-fraud efforts? .....	111
Q.2.29 If “YES” to Q.2.25, what specific functionalities of Arachne have proven most effective in your state’s fight against fraud? .....	111
Following Q.2.29, please specify "Other ". ....	111
Q.2.30 If “YES” to Q.2.25, are there procedures in place to address risk alerts generated by the Arachne system? .....	112
Q.2.31 If “YES” to Q.2.25, does your system have dedicated resources or a task force for handling the outputs and alerts generated by Arachne?.....	112
Q.2.32 Please feel free to share any additional thoughts or experiences you have regarding the topics discussed in this section. ....	113
Q.3.1 Have there been any changes in your anti-fraud governance structures in place in 2024? .....	116
Q.3.2 If “YES, we set up an anti-fraud governance structure” or “YES, we modified the existing anti-fraud governance structure” to Q.3.1, what are the key changes implemented?.....	117
Q.3.3 If “YES, we set up an anti-fraud governance structure” or “YES, we modified the existing anti-fraud governance structure” to Q.3.1, Which authorities have you newly included in your anti-fraud governance structures in 2024?.....	119
Following Q.3.3, please specify "Other" .....	120
Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure facilitates knowledge exchange and good practices to fight fraud.....	120
Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure is the ideal forum to elaborate a comprehensive risk assessment to support anti-fraud effort.....	120
Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure provides a comprehensive understanding of anti-fraud issues. ....	121
Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure contributes to the development / update of anti-fraud policies/strategies at the national level.....	121
Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure responds quickly to new threats in the anti-fraud environment.....	122
Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure contributes to drafting anti-fraud legislation.....	122
Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure contributes to the development and implementation of training to staff on anti-fraud.....	122
Polarplot of the Average Level of Self-Reported Governance Effectiveness in Anti-Fraud Efforts Across All Member States .....	124
Q.3.5 Could you describe any best practices or innovative methods that your anti-fraud governance structures have implemented to enhance effectiveness and collaboration? .....	124
Q.3.6 Has there been any change regarding the staffing of your national anti-fraud structure coordinating the anti-fraud governance (AFCOS) in 2024?.....	130
Following Q.3.6, please specify "Other" .....	131

Q.3.7 What are the main challenges currently faced in enhancing the anti-fraud governance in your Member State? .....	131
Following Q.3.7, please specify "Other". .....	131
Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6).: Increased funding / financial assistance .....	132
Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6).: Training programs for staff.....	132
Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6).: Facilitated cooperation initiative / sharing good practices among Member States .....	133
Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6).: Guidance on legal or regulatory framework adjustments .....	133
Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6).: Technological support.....	134
Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6).: Other (please specify in the following question) .....	134
Bar plot of the Average Level of Support Requested for Anti-Fraud-Policy Across All Member States.....	135
Q.3.9 If you selected “Other” to Q.3.8, please specify any other types of support you would need and its importance.....	135
Q.3.10 Please feel free to share any additional thoughts or experiences you have regarding the topics discussed in this section. ....	136
Q.4.1 Which national services were consulted to reply to this questionnaire?.....	137
Q.4.2 How could we improve this questionnaire? Please share any suggestions for enhancements or specific areas that could be improved for future iterations. ....	142



# Introduction

---

In its 2023 PIF Report the Commission made recommendations to Member States, covering: a) improving the reporting and follow-up of suspected fraud b) accelerating the digitalisation of the fight against fraud c) reinforcing anti-fraud governance in the Member States.

A specific questionnaire has been addressed to the Member States to collect information about how they have implemented these recommendations. Their replies are analysed in this document, which is divided in two parts: the first provides an overview and analysis of their replies, while the second part details, for each question of the survey, the specific replies given.

## Overarching Themes and Guiding Principle

Two central themes emerged from the Member States' responses. First, there was a strong call for more training modules and detailed guidance, highlighting the importance of training in addressing various challenges. Second, there was significant demand for enhanced collaboration and an exchange of best practices, both with OLAF and among Member States. This formed a guiding principle for the analysis. Where applicable, the analysis compiles best practices that Member States identified in addressing common issues to provide an overview of potential solutions.

# 1. Overview of Member States' replies to the questionnaire

---

## 1.1. *Recommendation 1: Improving the reporting and follow-up of suspected fraud.*

*The reporting and follow-up of suspected fraud can still be significantly improved. Member States should ensure that reported cases of suspected fraud are updated in a timely manner with reliable and complete information and data.*

*To this end, establishing appropriate communication channels with law enforcement and prosecution services; and exchanging information with investigative bodies and timely reporting are prerequisites to effective follow-up.*

*Complete reporting also implies that national authorities report irregularities and fraud detected by Commission audit services, the European Court of Auditors, OLAF and the EPPO as soon as the necessary information becomes available.*

### 1.1.1 Confidence in reporting systems

A significant majority of Member States showed a high degree of confidence in their reporting systems. 11 Member States<sup>1</sup> reported using a “well-established reporting system capturing all relevant data on suspected fraud cases and irregularities”, with 9 stating that they “have a strong reporting system but with some gaps in capturing all relevant data<sup>2</sup>”. Importantly, 17 Member States actively engage in regular reviews to assess the effectiveness of their reporting mechanisms<sup>3</sup>, underscoring a commitment to maintaining and improving system robustness.

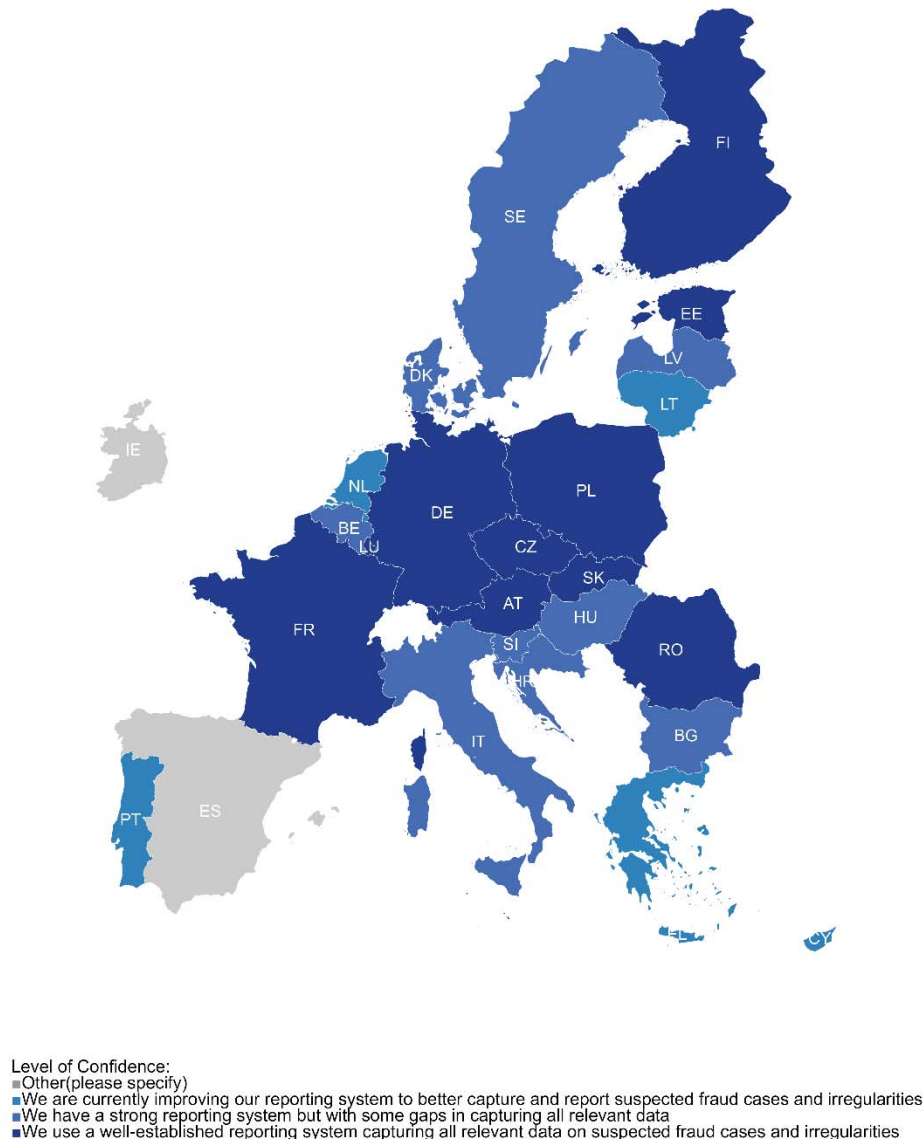
---

<sup>1</sup> Austria, Czechia, Estonia, Finland, France, Germany, Luxembourg, Malta, Poland, Romania, Slovakia

<sup>2</sup> Belgium, Bulgaria, Croatia, Denmark, Hungary, Italy, Latvia, Slovenia, Sweden

<sup>3</sup> Bulgaria, Cyprus, Czechia, Denmark, Estonia, Germany, Hungary, Italy, Latvia, Lithuania, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain

### Q.1.1 Self-Reported Confidence in National Reporting Systems



### 1.1.2 Issues with information flow

Member States have reported some persistent challenges. Some 13 Member States reported issues related to information flow<sup>4</sup>, commonly between judicial and reporting authorities. Problems often arise when judicial proceedings are prolonged, or investigation secrecy obstructs thorough reporting. These gaps can affect the timeliness and efficiency of follow-ups on reported cases. This communication issue emphasises the need for better collaborative measures and improved procedural clarity to ensure effective reporting systems across all governance levels. Notably, 17 Member States reported some improvement in their follow-up procedures over the past year<sup>5</sup>.

<sup>4</sup> Bulgaria, Croatia, Cyprus, Denmark, Estonia, Hungary, Lithuania, Poland, Portugal, Romania, Slovakia, Slovenia, Spain

<sup>5</sup> Bulgaria, Czechia, Denmark, Estonia, Germany, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Spain

### 1.1.3 Best practices mentioned by Member States

Member States identified the following best practices in addressing and preventing information flow difficulties:

- **Centralised Coordination:**
  - Establishing central contact points and specialized units to streamline communication between managing authorities, investigative bodies, and judicial authorities. This ensures efficient information flow and enhances interagency cooperation.
- **Comprehensive Guidelines and Systems:**
  - Developing detailed anti-fraud strategies and integrate national IT systems for monitoring and recording irregularities. Standardising procedures facilitates consistent data exchange across sectors and prevents knowledge loss during handovers.
- **Legal Frameworks and Obligations:**
  - Introducing legislation mandating information disclosure to prevent disputes between reporting and judicial authorities by establishing clear rules for information sharing. Such legal measures enhance transparency, create clear communication channels, and promote accountability.
- **Routine and Direct Communication:**
  - Encouraging regular and structured communication between authorities with designated contact persons. This approach promotes timely updates and flexible coordination, ensuring effective information sharing.
- **Collaborative Networks and Liaison Roles:**
  - Forming interagency networks and maintain liaison roles for ongoing dialogue with judicial authorities. These collaborations ensure comprehensive case follow-up and optimize oversight of suspected fraud and irregularities

## *1.2. Recommendation 2: Accelerating the digitalisation of the fight against fraud*

Digitalisation of the fight against fraud needs to be at the heart of anti-fraud strategies. As fraudsters increasingly use and exploit new technologies to commit crime, the EU anti-fraud architecture must be equal to the challenge to prevent, detect and investigate it.

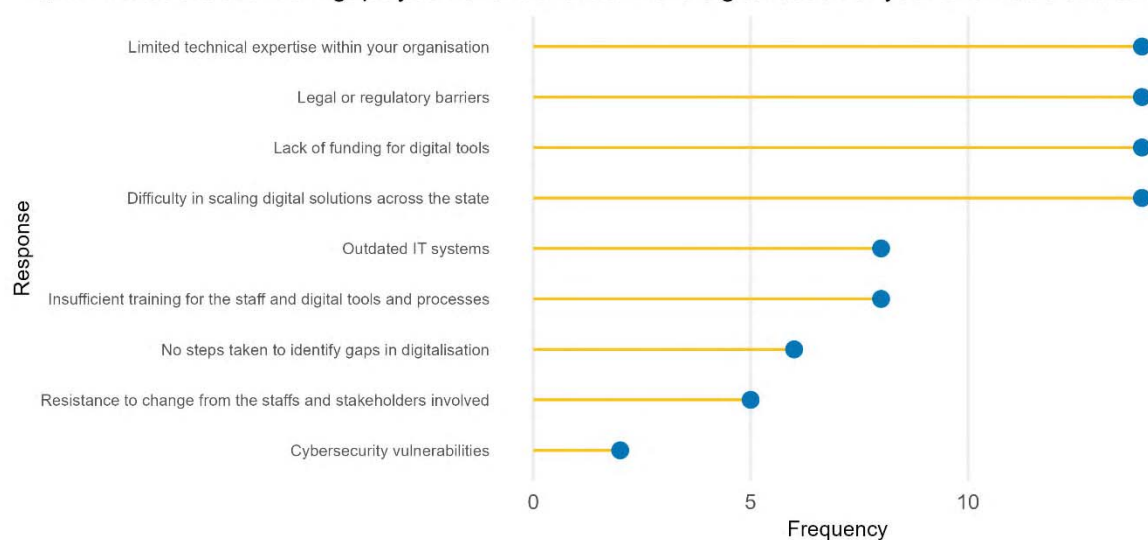
Member States should ensure that the digitalisation of the fight against fraud is part of their strategic approach to fighting fraud. Member States should begin their preparations for the next phase in the development of the Commission's risk scoring and data mining tool.

All Member States will be required to feed the tool with data as of the next multiannual financial framework. Such preparations could test the automated feeding of requested data and interoperability with national systems.

### 1.2.1 Current status and challenges in digitalisation

Digitalisation is a stated priority in all but two Member States<sup>6</sup> anti-fraud efforts. In contrast, only 6 Member States consider standardisation a crucial component of their digitalisation initiatives<sup>7</sup>. This indicates that although many are adopting digital tools, ensuring data is comparable across borders to improve fraud detection remains a lesser priority.

#### Q.2.4 What are the main gaps you have identified in the digitalisation of your anti-fraud efforts?



Member States for each response:  
 Cybersecurity vulnerabilities: CZ, RO  
 Difficulty in scaling digital solutions across the state: HR, SE, BE, LT, CZ, ES, DE, BG, CY, EE, RO, PT, LV, IT  
 Insufficient training for the staff and digital tools and processes: HR, NL, CZ, ES, SK, BG, RO, LV  
 Lack of funding for digital tools: HR, NL, GR, BE, FI, SI, CZ, ES, SK, DE, BG, EE, RO, LV  
 Legal or regulatory barriers: SE, NL, BE, LT, CZ, ES, SK, PL, DE, CY, EE, RO, LV, IT  
 Limited technical expertise within your organisation: LU, HR, SE, NL, GR, FI, CZ, ES, HU, SK, DE, BG, MT, RO  
 No steps taken to identify gaps in digitalisation: IE, FR, AT, SI, RO, DK  
 Outdated IT systems: LU, NL, GR, SI, CZ, ES, CY, RO  
 Resistance to change from the staffs and stakeholders involved: LU, HR, SE, CZ, BG

To address these gaps, Member States primarily rely on training, with 17<sup>8</sup> using it as their main approach to tackling deficiencies. Gap analysis and internal assessments are also used by 8 Member States<sup>9</sup> each. This shows a significant focus on capacity building and continuous evaluation to enhance digitalisation efforts and align with anti-fraud objectives.

<sup>6</sup> Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden

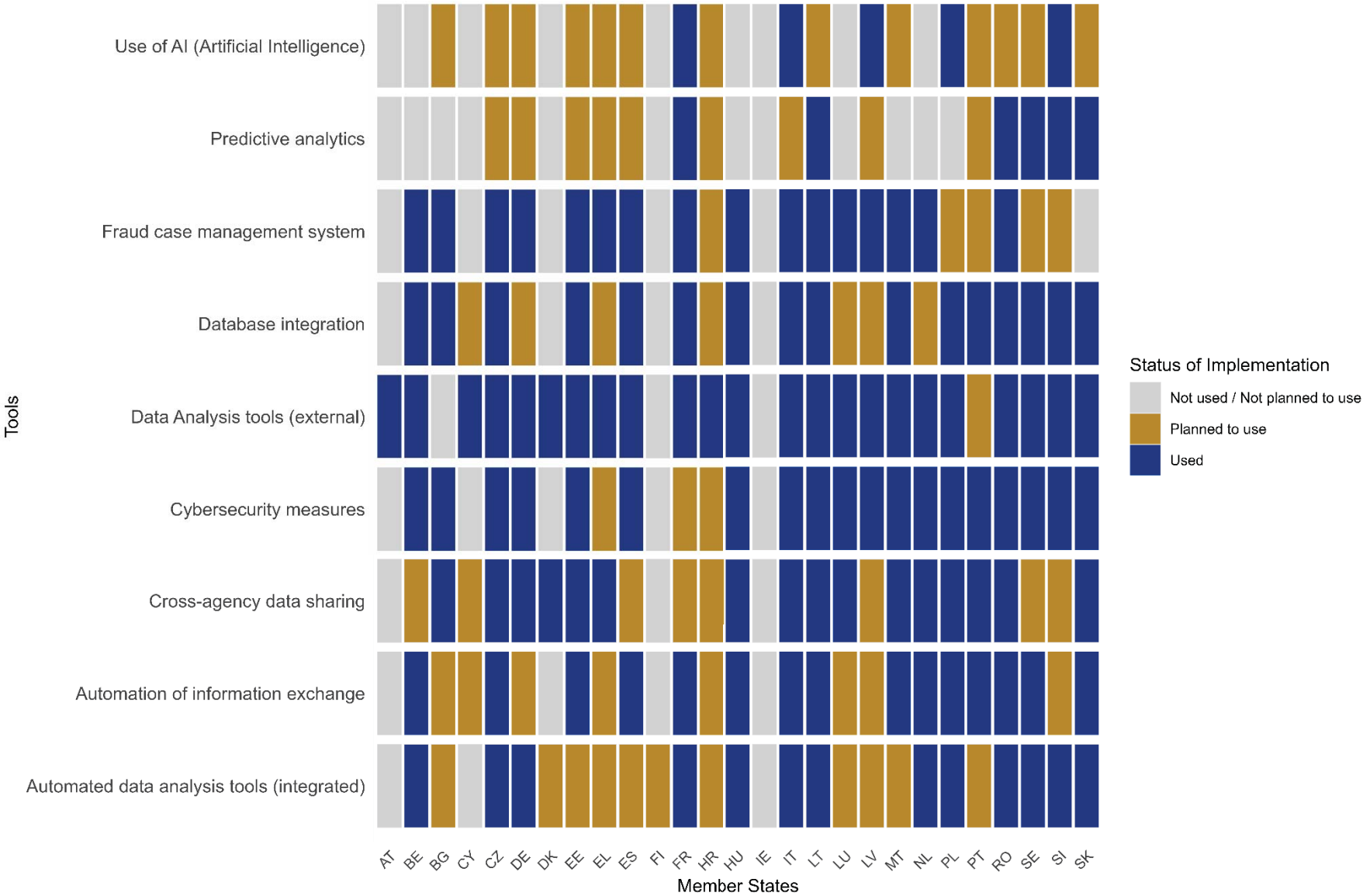
<sup>7</sup> Belgium, France, Italy, Malta, Portugal, Slovakia

<sup>8</sup> Austria, Belgium, Bulgaria, Cyprus, Czechia, Germany, Greece, Hungary, Italy, Lithuania, Malta, Romania, Slovakia, Slovenia, Spain, Sweden, Finland

<sup>9</sup> Internal assessment: Czechia, Denmark, Estonia, Germany, Greece, Italy, Luxembourg, Romania  
 Gap Analysis: Belgium, Czechia, Germany, Italy, Romania, Slovakia, Slovenia, Spain

Q.2.9 Which digital tools or technologies are currently in use?

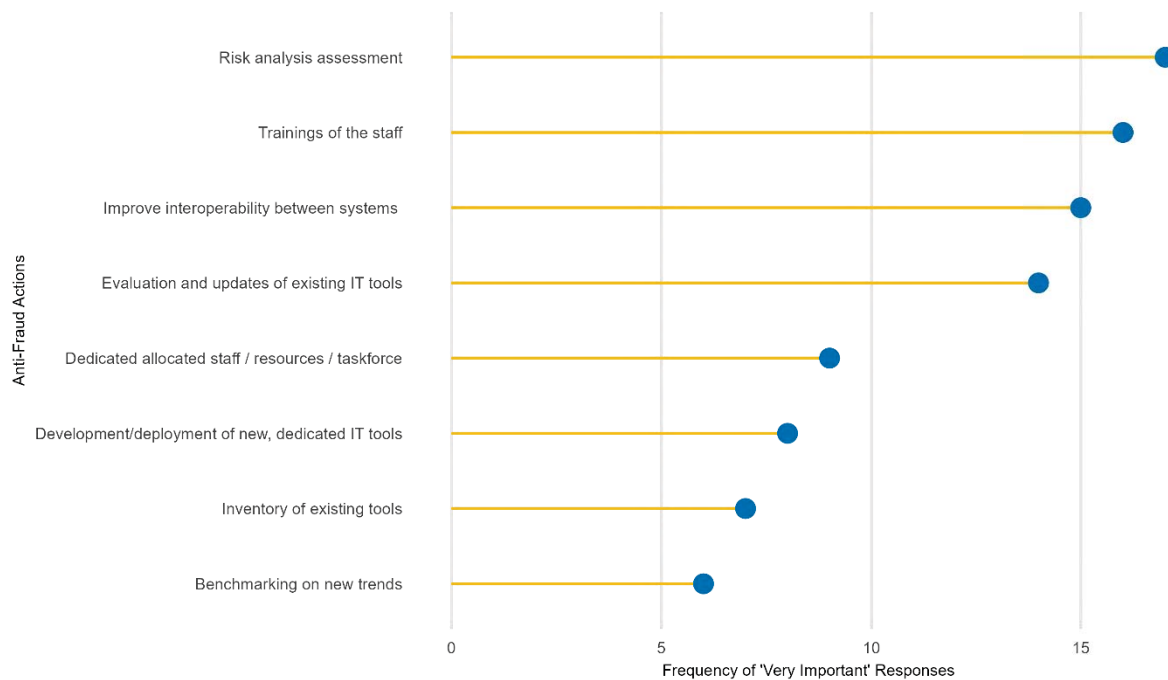
Digital Tools and Technologies



## Progress in digital transformation and it tool adoption among Member States

20 Member States report at least partial success in implementing IT tools<sup>10</sup>, marking significant progress in their digital transformation. The measures adopted reveal that Member States prioritise staff training, risk analysis, and the development of interoperable data systems, which are deemed vital for enhancing anti-fraud measures. Data analysis tools are widely used, with 24 Member States either already using or planning to use external and integrated data analysis tools<sup>11</sup>. Conversely, predictive analytics and AI are the least used digital tools in combating fraud, though AI is among the most planned for future use. Predictive analytics, currently underutilised, offers potential for optimising resource allocation and improving fraud detection efficiency.

Q.2.8 Frequency of 'Very Important' Responses Across Actions



## Interoperability advances and challenges in fraud detection systems

When examining the key challenges Member States face while digitalising their fight against fraud, two issues are most frequently cited: legal or regulatory barriers and data privacy and security concerns. The most mentioned challenges mainly relate to resource issues rather than a lack of commitment. This implies that while Member States are dedicated to digitalisation, certain obstacles hinder their progress rather than a lack of motivation.

<sup>10</sup> Partially successful: Austria, Belgium, Bulgaria, Denmark, Estonia, Finland, France, Greece, Lithuania, Latvia, Netherlands, Portugal, Slovakia, Slovenia, Spain, Sweden

Totally successful: Hungary, Italy, Malta, Poland

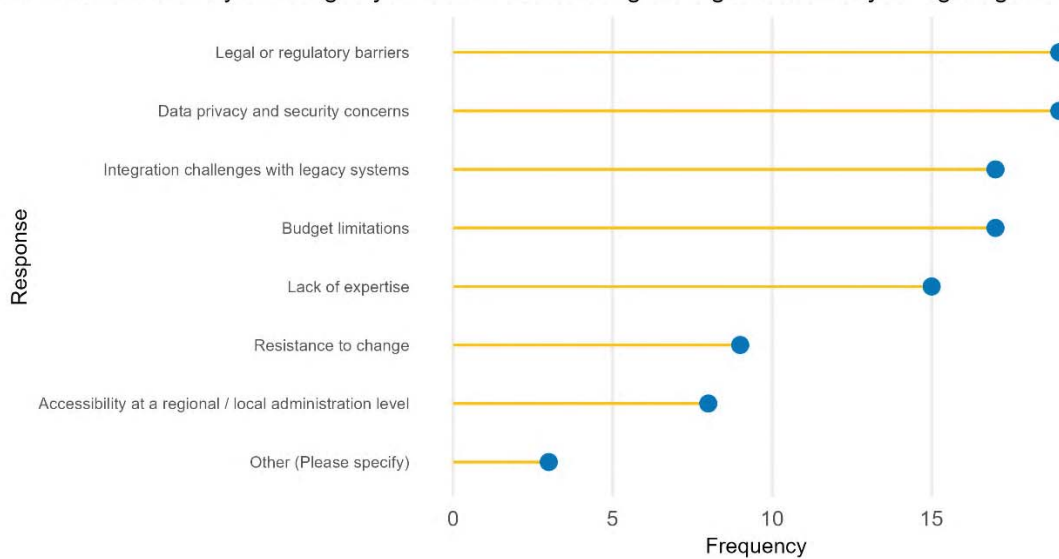
<sup>11</sup> External (In use): Austria, Belgium, Croatia, Cyprus, Czechia, Denmark, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Romania, Slovakia, Slovenia, Spain, Sweden;

External (Planned): Portugal

Integrated (In use): Belgium, Czechia, France, Germany, Hungary, Italy, Lithuania, Netherlands, Poland, Romania, Slovakia, Slovenia, Sweden

Integrated (Planned): Bulgaria, Denmark, Estonia, Finland, Greece, Latvia, Luxembourg, Malta, Portugal, Spain

## Q.2.17 What are the key challenges you face in accelerating the digitalisation of your fight against fraud?



Member States for each response:  
 Accessibility at a regional / local administration level: IE, HR, GR, BE, CZ, CY, RO, DK  
 Budget limitations: LU, HR, NL, GR, BE, FI, SI, CZ, ES, HU, SK, PL, DE, BG, EE, RO, LV  
 Data privacy and security concerns: IE, SE, NL, GR, BE, AT, FI, SI, CZ, ES, HU, SK, PL, DE, EE, RO, PT, DK, IT  
 Integration challenges with legacy systems: IE, LU, HR, NL, GR, BE, SI, ES, SK, PL, DE, BG, EE, RO, LV, DK, IT  
 Lack of expertise: LU, HR, NL, GR, BE, FI, SI, CZ, ES, HU, SK, DE, BG, RO, PT  
 Legal or regulatory barriers: IE, HR, SE, NL, GR, BE, FI, SI, CZ, ES, PL, DE, BG, MT, CY, EE, RO, LV, IT  
 Other (Please specify): SI, DE, RO  
 Resistance to change: LU, HR, GR, CZ, ES, BG, CY, RO, LV

While 16 Member States have developed interoperable data management systems<sup>12</sup>, 11 have not<sup>13</sup>. Achieving interoperability is essential for ensuring seamless data sharing and enhancing fraud detection mechanisms, highlighting an area for potential improvement and standardisation in future efforts.

<sup>12</sup> Austria, Belgium, Czechia, Estonia, France, Hungary, Ireland, Italy, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia

<sup>13</sup> Bulgaria, Croatia, Cyprus, Denmark, Finland, Germany, Greece, Latvia, Lithuania, Spain, Sweden



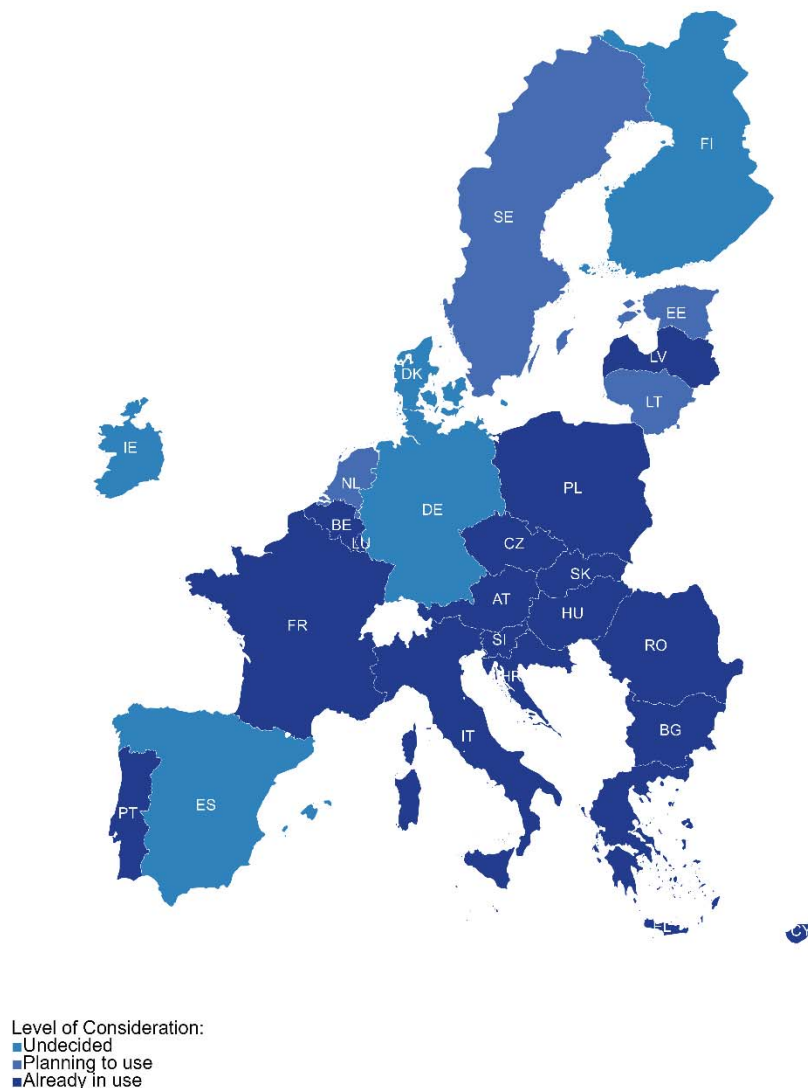
### 1.2.2. Approaches to achieve interoperability mentioned by Member States

Member States identified the following approaches to aid the interoperability of their data management systems.

- **Adopting standard protocols and frameworks:**
  - Using standardised protocols for data exchange.
  - Maintaining compliance with relevant industry standards.
- **Data integration and exchange:**
  - Establishing interfaces with external and internal systems for seamless data integration and automated exchange.
  - Enabling real-time data sharing across platforms.
- **Centralised information systems:**
  - Developing centralised data platforms that support multiple data formats.
  - Providing capabilities for generating both ad hoc and standardised reports.
- **Using of existing databases and registers:**
  - Integrating national registers and external databases for automatic data verification.
  - Ensuring automatic data retrieval and updates.
- **Data analysis and verification:**
  - Implementing systems for automatic cross-referencing and validation of data from multiple sources.
  - Using scoring models and algorithms to detect irregularities across various databases.

### 1.2.3. State-of-play and utilisation of ARACHNE

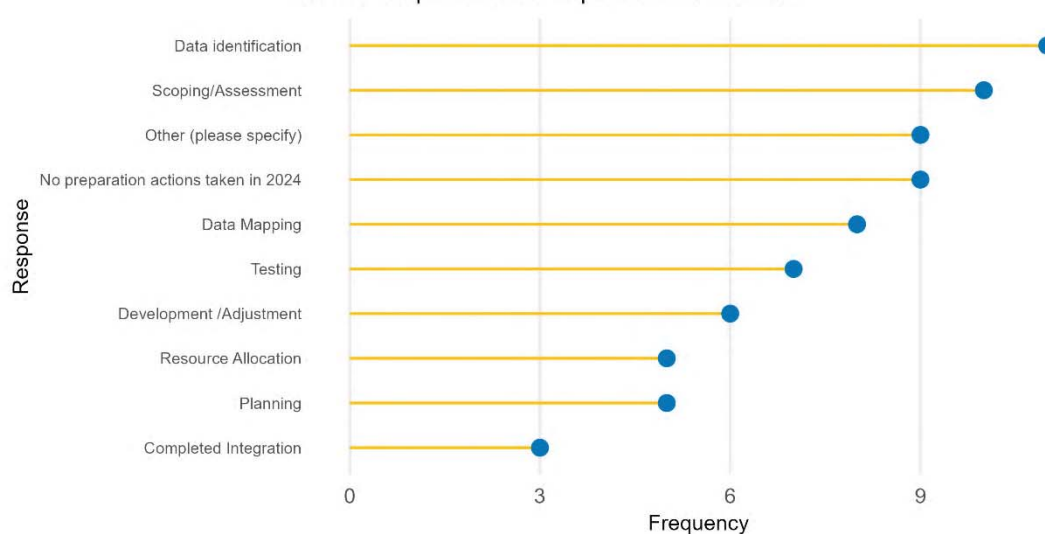
Q2.23 Are you considering the use of ARACHNE?



As the compulsory feeding of the data mining and risk scoring tool developed by the Commission draws closer, 22 Member States are using ARACHNE as part of their anti-fraud strategies<sup>14</sup>. Key actors in implementation are managing and auditing authorities. ARACHNE serves as a critical tool for detecting fraud and conflicts of interest, particularly within European Social Fund (ESF) procedural rules. It is extensively employed across various EU funds, including ESIF, RRF, and ERDF, where it aids mostly in prevention and detection through its risk scoring, profiling, and pattern recognition to identify potential fraud and irregularities. Despite its widespread adoption, Member States stress the need for comprehensive training and support to maximise the tool's effectiveness.

<sup>14</sup> Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Estonia, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain

## Q.2.20 Steps Taken to Implement ARACHNE



Member States for each response:  
 Completed integration: BE, HU, BG  
 Data identification: HR, BE, AT, SK, CY, EE, RO, PT  
 Data Mapping: HR, BE, ES, SK, BG, CY, EE, RO, PT, LV, IT  
 Development /Adjustment: BE, ES, SK, CY, EE, RO  
 No preparation actions taken in 2024: IE, HR, NL, FR, GR, FI, LT, SI, DE  
 Other (please specify): HR, SE, CZ, ES, SK, PL, MT, CY, RO  
 Planning: BE, ES, EE, RO, IT  
 Resource Allocation: BE, ES, CY, EE, RO  
 Scoping/Assessment: LU, BE, ES, SK, PL, CY, EE, RO, DK, IT  
 Testing: BE, SI, CY, EE, RO, LV, IT

## Integration challenges and data management issues with ARACHNE

Member States mentioned some difficulties integrating ARACHNE into national systems and showed varied adoption levels of the tool ranging from full integration to initial exploration. ARACHNE requires Member States to incorporate data from external databases or convert internal data into compatible formats, which imply potential interoperability issues and possible administrative burden. These issues about file-types to be used were commonly brought up by several Member States.

Half of the Member States reported moderate to significant improvements in their processes with ARACHNE<sup>15</sup>. Some difficulties remain in interpreting risk indicators and aligning outputs with the required scale of control. Legal clarity, especially concerning data protection, and continued improvements in system functionalities are key. Member States advocate for robust support mechanisms and adaptations to fully exploit ARACHNE's capabilities, in order for the system to meet the specific needs and challenges within each national framework.

<sup>15</sup>Moderate improvement: Austria, Belgium, Czechia, Malta, Portugal, Romania, Slovakia, Spain  
 Significant improvement: Cyprus, Greece, Italy

#### 1.2.4. Advantages vs difficulties with the use of ARACHNE

##### **Advantages**

*Integral tool:* The tool is recognised for effectively detecting fraud and conflicts of interest, especially in EU fund management verification processes.

*Cross-border fraud detection:* Effective in evaluating the risk of fraud, conflicts of interest, and irregularities, aiding compliance with financial regulations.

*Role in risk assessment:* Useful for monitoring risk categories and initiating further investigation when required.

*Supportive in national processes:* Assists countries in improving their control systems and effectively allocate resources to enhance fraud prevention and detection.

*Self-improving:* The tool becomes more efficient with increased usage and implementation.

##### **Common difficulties**

*Administrative burden:* Managing the tool requires significant effort, increasing administrative workload.

*Difficulties in interpretation:* Risk indicators and information may be difficult to interpret and may not align with necessary management controls.

*Data accuracy and updates:* Concerns are present over data reliability and timeliness which may lead to potential inaccuracies in risk assessment (false alerts).

*Compatibility with national legislation:* Challenges exist concerning compliance with data protection laws and public information access.

*Training and guidance:* More training modules and technical guidance is requested to reduce administrative burden.

### 1.3.Recommendation 3: Reinforcing anti-fraud governance in the Member States

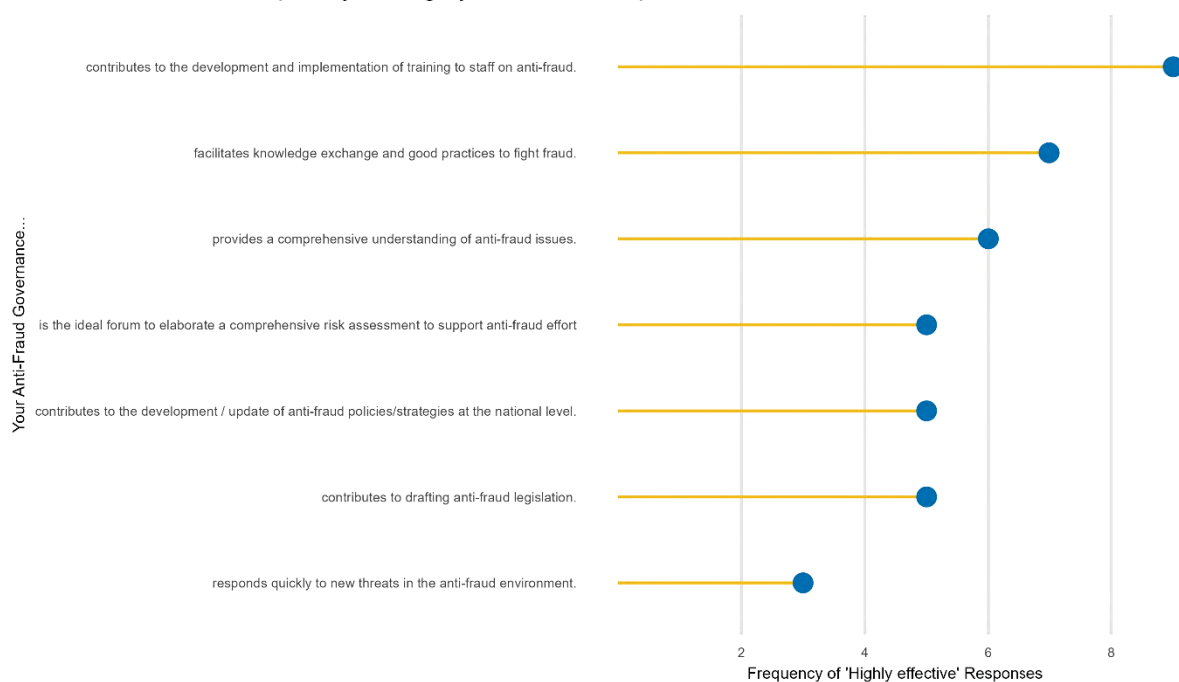
*Member States are requested to keep on reinforcing their anti-fraud governance structures, ensuring that they include all relevant players.*

*Central to this at Member State level is the adoption of all necessary strategies to fight fraud, ideally at national level (by adopting a national anti-fraud strategy).*

#### 1.3.1. State-of-play in national anti-fraud governance structures

Anti-fraud governance largely remains unchanged, with 74% of Member States noting no significant developments during the last year<sup>16</sup>. Governance frameworks typically need time to implement and evaluate new strategies and policies. However, Member States express high confidence in their anti-fraud governance structures. Among those Member States that did implement changes<sup>17</sup>, the focus was predominantly on enhancing the role and capabilities of Anti-Fraud Coordination Services (AFCOS). Enhanced cooperation and staff training are the types of support which Member States most frequently requested for improving their anti-fraud governance. Despite the static nature of current governance structures, Member States have identified several best practices aimed at strengthening their anti-fraud strategies.

#### Q.3.4 Frequency of 'Highly effective' Responses Across Governance Actions



<sup>16</sup> Austria, Belgium, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Lithuania, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Sweden

<sup>17</sup> Cyprus, Latvia, Luxembourg, Netherlands, Italy, Spain

### 1.3.2. Best practices in anti-fraud governance

- **Codified collaboration**

- Foster formal agreements and cooperation protocols to coordinate anti-fraud actions within and across borders. These collaborations enable shared best practices and enhance comprehensive monitoring and risk management.

- **Training and educational initiatives**

- Emphasise regular interactions and structured training among stakeholders. This strengthens anti-fraud efforts by enhancing information exchange, ensuring staff are well-prepared to tackle fraud-related challenges.

- **Comprehensive monitoring and documentation**

- Utilise digital technologies and centralised document systems to boost transparency and accessibility. These innovations facilitate efficient tracking and real-time data sharing, which are vital for effective oversight.

## 2. Responses from the Member States

Q.1.1 Have you reviewed the effectiveness of your reporting in the Irregularity Management System (IMS) in 2024?

Response	Frequency	Percentage	Member States
YES	17	63.0%	LT, SI, CZ, ES, HU, SK, PL, DE, BG, MT, CY, EE, RO, PT, LV, DK, IT
NO	10	37.0%	IE, LU, HR, SE, NL, FR, EL, BE, AT, FI

Q.1.2 If “YES” to Q.1.1, What were the main findings of your evaluation?

Member State	Response
LT	The evaluation identified that internal institutions in Lithuania are not sufficiently collaborating in terms of reporting and sharing information. As a result, there is a gap in communication and data exchange, which has affected the overall efficiency of the system. To address this issue, we are actively working on improving these processes to ensure better coordination and more effective information sharing between institutions moving forward
SI	Some institutions report YES, some institutions report NO.
CZ	Minor shortcomings in closure of cases.
ES	All the management authorities consulted answered no to this question, except one. In the case of the management authority that replied yes, the main finding was that the communications carried out have allowed for adequate monitoring
HU	The timeliness of recording the status of suspected fraud cases can be improved upon.
SK	AFCOS has reviewed the 2024 reporting effectiveness within the IMS internally, and the results are positive. We've identified some minor refinements to further improve efficiency.
PL	<p>The effectiveness of reporting in the IMS was verified in 2024 by AFCOS, which in Poland is responsible for organising and coordinating the process of reporting to the Commission irregularities found in the context of spending EU funds implemented under shared management. The results of this verification were described in an analytical document, which was submitted for appropriate use to the relevant national reporting institutions at the next two levels of the IMS reporting structure.</p> <p>The analysis covered the irregularities reported under the 2014-2020 financial perspective, and particular attention was paid to cases of (suspected) fraud, as well as the timeliness of reporting</p>

Member State	Response
	<p>irregularities. In order to obtain a horizontal view, the analysis also covered the closure status of the 2007-2013 PP cases in the IMS system.</p> <p>It showed that the reporting institutions continued to apply the good practices implemented with regard to whistleblowing, which had been developed and expanded over various financial perspectives. It was found that approx. 2000 reports of irregularities concerning the 2014-2020 PP remain open in the IMS due to ongoing investigations by law-enforcement authorities and time-consuming, challenging recovery proceedings. At the same time, many 2007-2013 PP cases remain open, which creates an additional administrative burden for the reporting institutions (the need for regular monitoring and appropriate action).</p> <p>AFCOS found the results of the analysis satisfactory: it was established that, as a general rule, the reporting deadlines were respected in relation to the primary administrative or judicial findings (PACA) and that the completeness of the data in individual cases remained high. AFCOS also issued appropriate recommendations to speed up efforts to bring cases from the previous financial perspectives to a close so that attention could be redirected to the 2021-2027 PP, which is already being implemented.</p>
DE	<p>As examples: The Schleswig-Holstein ERDF Managing Authority: Reporting functions reliably and effectively thanks to detailed provisions in the guidance on anti-corruption/anti-fraud measures and irregularities.</p> <p>The Saarland ESF Managing Authority: Reports of irregularities were followed up until the case was closed, and the comments of the BMS were taken into account and fed back. Corrections were made to cases. No cases of fraud.</p>
BG	<p>We prepared an Analysis of the reported irregularities for 2023 where we have made a statistical analysis of the reported fraudulent and non-fraudulent irregularities on national level and in the IMS. Also, we have made a review of the national procedures for administering of irregularities. The general conclusion is that the reporting system provides timely, correct and complete reporting of irregularities.</p> <p>The IMS is currently updated to include the new look and feel. After reviewing the reporting in the IMS in 2024, it was found that the reporting was done correctly, with filled in up-to-date and comprehensive information. The identified gaps are of a technical nature, due to the large volume of cases, and are being eliminated in a timely manner and within the work process. The reporting in IMS follows the reporting in Information System for Management and Monitoring EU Funds in Bulgaria 2020 (ISUN2020). The reporting in both systems is double checked by the AFCOS which tackles the mistakes that may occur. The reported cases of suspected fraud are updated in a timely manner with reliable and complete information and data.</p> <p>A control is introduced by a second Irregularity Officer and Supervising Manager in order to improve the irregularity reporting.</p>
MT	<p>The Maltese AFCOS already has effective reporting measures in place. In addition, in 2024, the Financial Investigations Directorate (FID) within the Internal Audit and Investigations Department (IAID), in its role as the Maltese AFCOS, has been strengthened with the recruitment of new personnel, who are primarily responsible for reporting of irregularities in IMS. This is ensuring that the four-eyes principle is always adhered to (IMS Creator inputs a case; IMS Manager finalizes the case).</p>



Member State	Response
	Once a case is closed, the Maltese AFCOS confirms that any data already inputted in IMS is correct by reconciling this data with the latest information received from the relevant Authorities.
CY	Issues with coordination between various entities regarding the status of cases, issues with timely reporting between entities.
EE	<p>Estonian AFCOS, as the IMS Country Officer, checks open cases in the IMS annually to follow the quality and continuity of reports and supports the reporting authorities with knowhow. Estonian Cohesion Policy Managing Authority regularly carries out checks on the reporting of irregularities to ensure whether the data is accurate. In general, the system works well, with minor errors occurring occasionally. Cases that have been referred to investigative bodies are more complex to report, as early-stage notification is often not possible. Premature reporting could jeopardize the investigation and subsequent criminal proceedings. For such cases, we await authorization from EPPO or the other investigative body before reporting.</p> <p>On a positive note, cooperation between the implementing agencies, the Managing Authority, and AFCOS is functioning, and we have an overview of the cases under investigation.</p>
RO	<p>- The Department for the Fight Against Fraud - DLAF: Communication is conducted in a timely manner, data completeness has been improved, solid cooperation with the reporting authorities.</p> <p>- Paying Agency for Rural Investments (AFIR): No deficiencies in the method of reporting irregularities or system deficiencies were detected.</p> <p>- The Ministry of Agriculture and Rural Development - Managing Authority for the Operational Programme for Fisheries and Maritime Affairs (DGP-AMPOPAM): Irregularities were reported in the IMS for all notifications and verifications of which the Managing Authority was aware. However, there were cases of delays in the information received from the institutions with audit/control functions concerning the submission of cases for investigation/verification to the judicial authorities. This then affected the reporting.</p> <p>- The Ministry of Energy: The suspected irregularities related to: (1) setting up project teams with overlapping tasks and activities, failing to respect the guide on the call for projects, (2) the legal regime governing documents, (3) the justification for co-financing.</p> <p>- The Ministry of Investments and European Projects (MIPE) – Directorate-General for Sustainable Development Programmes (DGPDD): The effectiveness of reporting was found to have improved, due to the updating of operational procedures, the frequency of use of prevention tools, and the performance of fraud risk assessment.</p> <p>- The Ministry of Investments and European Projects (MIPE) – Managing Authority for the Human Capital Operational Programme (MA POCU): The reporting system has been improved compared to the version from the previous year. The criteria for filtering previously notified irregularity reports do not allow for identification using the internal reference number. The history of irregularity reports by operational programme can be consulted only by exporting the data available on each page viewed.</p>
PT	As regards the irregularities related to the Cohesion Policy Funds in the 2014-2020 PP, there was some delay in the reporting to OLAF. Procedures are being reviewed to improve coordination and the timely reporting of irregularities.
LV	For the Ministry of Agriculture and Rural Support Service: The reporting process is working. Reports are submitted complete in terms of content, updated in a timely manner where necessary

Member State	Response
	with reliable and complete information and data, and submitted within the specified deadlines. Information exchange and cooperation between institutions is working and continuously developing. Communication channels (official correspondence) and operational communication are appropriate.
DK	<p>Most of the contributions to the survey reported a “No” in Q.1.1.</p> <p>The Danish Agency for Green Land Conversion and Water Environment reported “Yes” and noted: The reporting authority performs ongoing quality checks of our reporting to make it uniform and complete.</p>
IT	<p>The review of the Irregularity Management System (IMS), performed on an ongoing basis by the national liaison officers, gives an essentially positive picture as regards the consistency, completeness and correctness of the data. This is primarily thanks to continuous analysis, monitoring and control of reports, carried out at central level in close connection and consultation with the managing authorities, both when reports are sent and when they are updated.</p> <p>For example, it is worth passing on the information received from the Ministry of Education and Merit, within whose remit, in 2024, the MA for the NOP/NP ‘School’ reported 5 cases to the IMS, classifying them as IRQ2 ‘irregularities’. In compliance with the [national] ‘Guidelines on how to notify the European Commission of irregularities and fraud against the EU budget’, the reports in question were preceded by careful internal investigations. These took account of the findings of the inspections ordered, the on-the-spot checks carried out at beneficiaries, the details obtained following dialogue with beneficiaries, and the information obtained via feedback from external control bodies so as to ascertain whether any criminal proceedings were ongoing for suspected criminal offences against the EU budget in respect of the NOP ‘School’ projects being examined. The reports can thus be considered effective as they are complete, timely, detailed and reflect the findings of all the checks carried out.</p>

### Q.1.3 How would you evaluate your level of maturity of your current reporting process for reporting irregularities and, in particular, fraud?

Response	Frequency	Percentage	Member States
We use a well-established reporting system capturing all relevant data on suspected fraud cases and irregularities	11	40.7%	LU, FR, AT, FI, CZ, SK, PL, DE, MT, EE, RO
We have a strong reporting system but with some gaps in capturing all relevant data	9	33.3%	HR, SE, BE, SI, HU, BG, LV, DK, IT
We are currently improving our reporting system to better capture and report suspected fraud cases and irregularities	5	18.5%	NL, EL, LT, CY, PT
Other (please specify)	2	7.4%	IE, ES

Following Q1.3, please specify "Other".

Member State	Response
IE	The vast bulk of expenditure is incurred initially via the Central fund/Vote management process and comes under the anti-fraud policy of the relevant Department. It is subject to audit by the Comptroller and Auditor General and where any instances of irregularities are discovered they are reported where required and excluded from the payment application submitted to the European Commission. Fraud and suspected fraud are reported as required.
ES	Some managing authorities have replied 'We use a well-established reporting system capturing all relevant data on suspected fraud cases and irregularities' while others have replied 'We are currently improving our reporting system to better capture and report suspected fraud cases and irregularities'.

Q.1.4 Can you provide examples of well-established reporting systems or practices that have been effective in capturing and reporting suspected fraud cases and irregularities?

Member State	Response
IE	All fraud and suspected fraud cases are reported using the IMS. All payments are checked by the MAs and where an irregularity is found the case is removed from the payment claim.
LU	Prior checks, ex-post checks, regular risk analysis and follow-ups in addition to support/guidance for beneficiaries.
HR	<p>Contribution from Ministry of Finance, Tax Administration:</p> <p>The Tax Administration has a special Unit that cooperates with the European Public Prosecutor's Office (further in the text: EPPO) and other criminal prosecution bodies on investigations (Independent Sector for Financial Investigations).</p> <p>Contribution from AFCOS unit:</p> <p>AFCOS unit drafts Irregularity Management Guidelines that contain procedures describing proceedings in the area of prevention and detection of irregularities; proceedings related to suspicions of irregularities and identified irregularities, reporting on irregularities and follow-up of reported irregularities in the context of management and control of using EU funds. The objective of the Guidelines is to develop consistent practice in applying legal framework for the protection of European Union financial interests and to ensure high quality of irregularity reports.</p> <p>Furthermore, AFCOS unit performs check of technical correctness of irregularity reports sent by Management and Control system bodies (further in the text: MCS bodies). If errors and/or omissions are detected during such a check, AFCOS unit rejects such reports, and it provides instructions for modification / correcting the report.</p> <p>Finally, AFCOS unit provides trainings on the use of IMS. There are basic one-on-one trainings intended for each new IMS user during installation of IMS certificate, consultations with current users and periodical trainings for a larger number of trainees (e.g. employees of MCS bodies for a certain programme). Finally, user support in the form of phone consultations is ensured at any time.</p>
SE	Irregularities and suspected fraud are detected during project audits and controls. The authorities have an expert function in support of administrators, covering compliance and the countering of

Member State	Response
	irregularities. Case handlers responsible for payments are required to report recoveries, and any recoveries decided on are followed up. It is also ensured that suspected fraud cases are reported.
NL	n/a
FR	For CAP funds, agricultural irregularities are reported to the Secretariat of the CICC EAGF by the four paying agencies (ASP, FRANCEAGRIMER, ODARC and ODEADOM). The data are checked carefully by the bodies responsible, then forwarded to the Secretariat to be verified, coordinated and validated.
EL	Recovery and Resilience Facility Coordination Agency (RRFA): Regulation (EU) 2021/241 does not require Member States to use the Irregularity Management System (AFIS/IMS) to report irregularities found in Recovery and Resilience Facility projects to the European Commission. Nevertheless, relevant information is sent to OLAF by email, setting out all the relevant data concerning the irregularities or suspected cases of fraud as referred to in the Irregularity Management System (IMS). In any case, it should be noted that to date, no irregularities giving rise to the suspicion of fraud have been detected.
BE	ERDF, JTF and RRF at the SPW (Walloon Public Service): The OLAF working group meets quarterly. It is charged by the Walloon government with reporting irregularity cases to OLAF where this is required or reporting an absence of irregularity cases, pursuant to EU rules and with reference to the European Development Fund (ERDF), the Just Transition Fund (JTF) and Wallonia's parts of the National Recovery and Resilience Plan (NRRP) and the Brexit Adjustment Reserve (BAR). The working group is made up of members representing the various administrations responsible. Minutes are taken of all OLAF working group meetings. These set out the proposals put to the working group members for examination, and, for in-person meetings, the decisions taken by the working group, as well as all the related documents sent to all members following the meeting. The secretariat reports irregularities to OLAF electronically. If, for the period concerned, there are no irregularities that need to be reported, the secretariat also reports this fact to OLAF electronically. Suspicions of fraud involving criminal offences are passed on to the Belgian judicial authorities.
AT	The Federal Ministry of Agriculture's IMS reporting system focuses on recoveries made by the Paying Agency and determines their causes on a case-by-case basis.
FI	<p>The intermediate bodies for the EU's regional and structural policy programme systematically record all suspected fraud and other observations in the programme's EURA 2021 information system.</p> <p>During the training organised for the intermediate bodies by the managing authority for regional and structural policy, the importance of a low threshold for reporting crimes was emphasised. Where necessary, the intermediate body also reports suspected fraud to the European Public Prosecutor's Office (EPPO) in accordance with the instructions the EPPO provides. Where required, the managing authority provides the intermediate bodies with support and guidance in cases of suspected fraud. The central authorities responsible for the management and control of programmes are responsible for reporting via the Irregularities Management System (IMS).</p>
LT	One example of an effective reporting system in addressing suspected fraud and irregularities is the strengthened collaboration between the European Union (EU) funds management agencies and the Financial Crime Investigation Service (FCIS) in Lithuania. This partnership aims to ensure timely receipt of information and proper processing of data. By fostering better communication and

Member State	Response
	coordination between these institutions, the system improves the detection and reporting of irregularities and fraud related to EU funding, enhancing overall effectiveness and responsiveness in combating financial crimes
SI	no
CZ	Carefully developed methodological environment within each programming period, national monitoring systems, centralised recording.
ES	<p>(1) The existence of irregularities may be detected by any of the bodies involved in the management of the funds and will in all cases be recorded in their FAMI III (formerly FAMI II) application, prior to the relevant communication to the Commission.</p> <p>(2) The authority which has definitively established the existence of the irregularity to be reported to OLAF shall register it in the IMS (Irregularities Management System). Once the irregularity has been reported in the IMS system, the relevant box shall be ticked in the FAMI III application.</p> <p>(3) The Control Unit shall be responsible for the follow-up of reported irregularities and, where appropriate, related administrative and judicial proceedings and shall keep the Managing Authority and the Intermediate Body informed so that they can take the necessary fraud risk management measures.</p>
HU	There has been long-standing and successful cooperation between national reporting organisations and Anti-Fraud Coordination Services (AFCOS). AFCOS organises quarterly meetings for the Irregularity Reporting Working Group with the participation of national reporting bodies (Managing Authorities, Certifying Authority, Paying Agency and judicial bodies) to support reporting in IMS. AFCOS also provides practical IMS training on reporting obligations and experience to Hungarian users on an annual basis. These measures form an important element of the action plan for an anti-fraud and anti-corruption strategy for EU funds.
SK	The Slovak republic has a well-functioning national information system (ITMS/ITMS2014+/ITMS21+) for Cohesion policy. According to the national law, the Managing Authority and the Intermediate Body are required to provide information about any irregularities and their updates within 15 working days. Among the typical qualification of irregularities (IRQ2, IRQ3 and IRQ5), we have also introduced an additional identification SIG “signal of irregularity”, which represents an initial detection of a violation. At this stage, the irregularity is already recorded in the national information system. This indicator SIG helps us, at the national level, to improve the detection and reporting of irregularities. Another well-functioning system for collecting data in the agricultural funds is AGIS MFR information system. The reports from these systems are inserted into IMS. JEMS - IT system is another IT tool for Interreg used at the national level which collects data of the beneficial owner data.
PL	Under the Code of Criminal Procedure, central and local-government institutions in Poland (including the institutions of the management and control system for EU funds) are legally obliged to report to the law enforcement authorities criminal offences prosecuted ex officio where such offences are detected by those institutions in the course of their activities. Reporting an offence may give rise to an investigation or inquiry. When reporting a criminal offence, it is necessary to provide evidence to substantiate the suspicion, which is why the reporting institutions make their own findings, taking into account the information and data identified, including data from dedicated IT tools supporting the fight against fraud. Where applicable, information on suspected fraud and on

Member State	Response
	<p>the involvement of law enforcement authorities is reflected in the IMS, in accordance with the rules resulting from the relevant EU sectoral regulations and the national procedure that has been designed in line with those regulations.</p> <p>An example of good practices ensuring that cases of suspected fraud are reported to the Commission is the cooperation agreement between the National Public Prosecutor and the Minister responsible for regional development, which regulates the provision of information on ongoing and concluded proceedings concerning projects co-financed by European funds. On the basis of that agreement, there is a regular exchange of data on the beneficiaries of EU funds against whom investigative measures have been taken, and some institutions also make use of the possibility to directly contact the designated representatives of the Public Prosecutor's Office where it is necessary to obtain data on ongoing proceedings without delay.</p> <p>Examples of solutions that have been implemented in Poland also include:</p> <ol style="list-style-type: none"> <li>1. agreements on the transmission to the organisational units of the Central Anti-Corruption Bureau, by means of distance communication, of information collected in the ICT systems SL2014 and CST2021 supporting the implementation of the programmes;</li> <li>2. cooperation agreements between the Minister responsible for regional development and the Agency for Restructuring and Modernisation of Agriculture (the Paying Agency) concerning cooperation: <ol style="list-style-type: none"> <li>(a) as regards the implementation of cross-checks aimed at detecting and eliminating double financing of cohesion policy expenditure and agricultural and fisheries programmes under the 2014-2020 PP;</li> <li>b) as regards the exchange of data on beneficiaries implementing projects/operations/actions in programmes under: Cohesion Policy 2021-2027, the European Funds for Fisheries Programme and the Strategic Plan for the Common Agricultural Policy 2023-2027 (CAP SP);</li> <li>c) as regards the implementation of cross-checks aimed at detecting and eliminating double financing of expenditure under SP, FERS and the CAP SP;</li> </ol> </li> <li>3. granting designated OLAF and EC staff access to the SL2014 main application in order to enable independent analysis of information on applicants, beneficiaries, expenditure items being settled and checks;</li> <li>4. the Paying Agency's procedures to ensure the collection and use of fraud-related data (dedicated databases that allow the recording of suspected and proven fraud cases, operated by all organisational units of the Agency and entities performing delegated tasks which are involved in the detection of irregularities and fraud; the data collected significantly facilitate the analysis, investigation and prevention of detected and suspected fraud cases).</li> </ol> <p>All these arrangements are effective in contributing to detecting cases of irregularities, including cases of suspected fraud (which results in reports being submitted to the Commission, where appropriate).</p>
DE	<p>In general:</p> <p>Drawing on IMS data findings and the corresponding explanations from the reporting bodies; regular exchanges with the managing and audit authorities. Below are examples from the competent ministries and ERDF authorities:</p> <p>The Federal Ministry of Labour and Social Affairs (BMAS): In the context of the European Social Fund Plus (ESF Plus), there is a guidance document for the ESF Plus Federal Programme which deals with the reporting of irregularities (including suspected cases of fraud). Under the ESF Plus</p>



Member State	Response
	<p>Federal Programme, cases are examined by the managing authority and the intermediate managing bodies. Where necessary, the managing authority instructs the relevant granting authority to take action, which may include, in particular, an on-the-spot check. The granting authority sends an IMS report to OLAF and, where necessary, notifies the offence to the national public prosecutor's office or the European Public Prosecutor's Office.</p> <p>The Bremen ERDF Managing Authority: The intermediate bodies implement operations. Potential cases of fraud are reported to the managing authority while, at the same time, detailed checks are carried out in order to either confirm or dispel the suspicion of possible fraud. If the suspicion of fraud is confirmed, the intermediate body in turn notifies the managing authority and the public prosecutor's office.</p> <p>The Lower Saxony ERDF Managing Authority: Direct reporting to law enforcement has proven effective. Furthermore, the establishment of the Investitions- und Förderbank Niedersachsen (NBank) has proven to be the only intermediate body. The centralisation of the implementation of all EU funding programmes to only one body guarantees the proper fulfilment of the tasks assigned and a sustainable flow of information.</p> <p>In addition, the retention of the 100% verification of supporting documents contributes to a significant reduction in the number of suspected fraud cases within the framework of the calls for funds. The Schleswig-Holstein ERDF Managing Authority: Communication channel with the public prosecutor's office; timely reporting of any suspicion, backed up by legal expertise.</p>
BG	<p>The national reporting system is based on the rules of the National regulation for administering irregularities and the Methodological guidelines for administering irregularities issued by the AFCOS Directorate. They transfer on the national level the EU regulations, the Handbook on reporting irregularities in shared management and the IMS manuals. The effective work of the national reporting system is guaranteed by regular trainings for the irregularity officers and a regular control of the compliance with the rules by the AFCOS Directorate.</p> <p>For instance, in cases of suspected fraud, after performed administrative proceedings on submitted signal for irregularity the "Territorial Cooperation Management" (TCM) Directorate at the Ministry of Regional Development and Public Works (MRDPW) is obliged to send the case to the Prosecutor's Office.</p> <p>After performed investigation the TCM Directorate is informed about the prosecutor's decision whether there are/ are not enough grounds to open an investigation or abandons an investigation that has been opened.</p> <p>Our reporting system contains clearly defined rules and processes with specifically named responsible persons for every task. There are check-lists to ensure rightful completion of the tasks.</p> <p>We report fraud cases and irregularities in 1-month period after every quarter in both ISUN2020 and IMS. We are also kept in touch with the prosecutor office every 6 months for decisions on fraud cases.</p> <p>When the need arises, joint inspections are carried out with the AFCOS Directorate at the Ministry of Interior; Methodological instructions are provided by the AFCOS Directorate for the administration of irregularities; Position from the AFCOS is given, including by phone/e-mail on the correct proceeding with the administration of irregularities;</p> <p>The AFCOS Directorate gives instructions on the correct entry of information into IMS; Trainings for irregularity staff conducted by the AFCOS Directorate is available, regarding operations with IMS and administration of irregularities.</p>

Member State	Response
	<p>The Prosecutor's Office of the Republic of Bulgaria (PORB) is a key institution in the fight with crimes against the EU's financial interests in Bulgaria.</p> <p>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 (at that time) was established in order to organize and ensure the interaction between the Prosecutor's Office of the Republic of Bulgaria (PORB) 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.</p> <p>The fore-mentioned department 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 and reporting with all national and international partners in the field.</p> <p>All strategic analysis and targeted reports from the Commission, OLAF, EPPO, etc. are received, analysed, taken into account and practically implemented according to the competences of the Prosecutor's Office. Cooperation agreement on interaction and cooperation between the Prosecutor's Office of the Republic of Bulgaria and the Ministry of Interior in countering offenses affecting the EU's financial interests was signed on 11.06.2024.</p>
MT	<p>The Maltese AFCOS receives all irregularity reports from the Managing Authorities of EU Funds on a quarterly basis, which reports are reviewed based on standing regulations and guidelines.</p> <p>On a quarterly basis, the Maltese AFCOS also holds the Irregularity Reporting Sub-group meeting with the Managing Authorities of EU Funds, Audit Authority and Paying Agency to ensure the correct reporting of irregularities to OLAF via IMS.</p>
CY	<p>Under selected shared management programs there is an automated process when documenting an irregularity to indicate the requirement to complete an irregularity report. For Cyprus Agricultural Payment Organisation- The reporting system is integrated into the information systems used by CAPO for administrative checks and in the accounting information system. Data can be retrieved and accessed automatically.</p> <p>Main weaknesses arrive from non-shared management programs/direct management from Commission/Territorial Cooperation programs where more than one MS authorities are involved.</p>
EE	<p>In our national grants information system, each project has a module for irregularities where information about specific project-related irregularities is entered, if necessary, with the same level of detail as the information reported to OLAF. All cases of suspected irregularities or fraud are recorded from the first euro cent, and the information remains even if it is later determined during the proceedings that no irregularity or fraud has occurred. Estonia uses a single grants information system that encompasses projects from various funds (ESI Funds, RRF, Norway/EEA, AMIF/ISF national support etc), enabling the implementing agency to check whether the beneficiary has had any irregularities and what kind. The same information system has been in use for several programming periods, allowing us to also see irregularities from previous periods.</p> <p>We have a similar reporting system for AGRI/FISH funds too. We have created a possibility to perform cross-checks between these two systems. The persons who have right to do cross-checks</p>



Member State	Response
RO	<p>can see whether the beneficiary has irregularities in other system. For more details they must communicate with the owner of this project.</p>
	<p>- DLAF: Clear reporting regulations. Obligation to designate an irregularity officer in the reporting authority. Solid cooperation with the reporting authorities and continuous training of staff involved. Interinstitutional cooperation protocols. Operational irregularity reporting network.</p> <p>- The Ministry of Energy: REGAS platform, ARACHNE platform.</p> <p>- MIPE – DGPDD - Reporting of all cases of suspected fraud recorded in the RD and in the other records specific to the activity of detecting irregularities and fraud, in accordance with operational procedures.</p> <p>- MIPE – Directorate-General for Health Programmes (DGPS): A communication channel with the National Anticorruption Directorate (DNA) has been created (contact person at MIPE level and exchange of information from a specific e-mail address through the contact person), since the exchange of information with the national investigative authorities and timely reporting are prerequisites for effective monitoring.</p> <p>- MIPE – Directorate-General for Management of the Recovery and Resilience Facility (DGMMRR):</p> <p>A) Reporting based on controls by the National Coordinator the Audit Control, Recovery and Monitoring Service of the DGMMRR performs the following activities:</p> <p>1. The control mandate is issued in the event of confirmation of the suspicion of irregularity/serious irregularity/ whistleblowing, where this is confirmed on the basis of checks carried out in light of the aspects included in OP DGMMRR No 10- ‘Checklist for suspensions of irregularity/fraud and mandate approval’. The persons included in the control mandate must make declarations concerning: - the absence of conflict of interest, - impartiality and confidentiality.</p> <p>2. If there is a notification regarding a suspicion of fraud and if this is confirmed by the checks carried out on the checklist included in Procedure No 10, the control mandate will be issued. Based on the control findings and if the suspicion of serious irregularity is confirmed by the evidence, the control team applies Government Emergency Ordinance No 70/2022, as amended, in which case the control body will notify the DLAF/OLAF, EPPO/DNA or other relevant prosecution authorities as soon as possible (immediately).</p> <p>B) Reporting based on controls by the reform and/or investment coordinators through the National Coordinator in line with the following provisions:</p> <p>i) EMERGENCY ORDINANCE No 70/2022 on the prevention, verification and detection of irregularities/double funding, and serious irregularities found in obtaining and using external grants and loans allocated to Romania through the Recovery and Resilience Facility and/or national public funds related to them and the recovery of the resulting debts, ii) EMERGENCY ORDINANCE No 124/2021 establishing the institutional and financial framework for the management of European funds allocated to Romania under the Recovery and Resilience Facility and amending and supplementing Government Emergency Order No 155/2020 on certain measures for drawing up the National Recovery and Resilience Plan necessary for Romania to obtain external grants and loans under the Recovery and Resilience Facility. The reform and/or investment coordinators provide immediate/quarterly notification through (the Register of suspected irregularities/fraud and debtors) the specialised control body within the MIPE - the National Coordinator (NC) of referrals made by the bodies it coordinates and their result (debt securities/debt recovery notes), or whenever the NC</p>

Member State	Response
	<p>so requests, concerning the status of the recovery of budget debts/the finalisation of the recovery process.</p> <p>- Ministry of the Environment, Water Resources and Forestry (MMAF): Reporting of all cases of suspected fraud recorded in the RD and in the other records specific to the activity of detecting irregularities and fraud, in accordance with operational procedures.</p>
PT	The information system aggregating the results of administrative checks, on-the-spot checks and audits in the context of the collection, storage, processing and reporting of irregularities and suspected fraud cases has been optimised.
LV	There are no specific examples.
DK	<p>The Danish Business Authority reported that potential whistleblowers have the opportunity to make contact and draw attention to a situation anonymously by making use of a whistleblower scheme.</p> <p>The managing authority makes use of an external auditor that is obliged to tell the managing authority if they encounter a case of possible fraud.</p>
IT	<p>At the start of 2024, the Guardia di Finanza Unit for Combatting Fraud against the European Union, as technical secretariat of the Committee for Combatting Fraud against the European Union (COLAF), issued all managing authorities with specific 'Guidelines for improving the procedures for filling in/populating irregularity/fraud reporting forms in the IMS'. The aim of these guidelines was to improve the quality of the information in the IMS. Specifically, the guidance concerned:</p> <ul style="list-style-type: none"> <li>a. how to create, save and finalise irregularity/fraud reporting forms, with specific reference to populating the various fields correctly, fully and consistently;</li> <li>b. the timescales for updating cases as new developments occur;</li> <li>c. details of case types in previous programming periods;</li> <li>d. drafting of the special report in cases where sums to be charged to the EU budget are irrecoverable;</li> <li>e. updating of cases in the system that have already been closed (e.g. owing to decertification, total recovery, etc.) but for which the associated judicial/administrative/accounting proceedings are still ongoing;</li> <li>f. close monitoring of all cases in the system in which the judicial authorities are known to be involved.</li> </ul> <p>In addition, should difficulties arise in any dialogue with the judicial authorities, the competent managing authorities have been given permission to immediately contact the aforementioned Guardia di Finanza Unit, which will provide support including, where possible, by facilitating contact with the prosecutors or judges involved. These guidelines have helped to make the reporting of suspected fraud and irregularities more effective.</p> <p>To use the example of a specific case, the MA of the Ministry of Education and Merit's NOP/NP 'School' has stated that the system for detecting and subsequently reporting irregularities or suspected fraud is composed of various stages that can be concisely summarised as follows:</p> <ul style="list-style-type: none"> <li>- detection: via ordinary first- and second-level checks, checks by higher-ranking control bodies, checks ordered following reports from third parties (e.g. complaints, reports, news stories, etc.);</li> <li>- assessment and examination of cases detected through e.g. specific on-the-spot checks, inspections at beneficiaries' premises by the competent Regional Education Department (USR), and procedures</li> </ul>

Member State	Response
	for dialogue and information exchange with external control bodies where information has been received on possible relevant ongoing criminal proceedings; - reporting: a report is made once the checks ordered have been completed, if conditions requiring the MA to make a report are fulfilled.

Q.1.5 Have you identified in 2024 new weaknesses in your reporting practices that could hinder the timely and exhaustive reporting in IMS, in particular of suspected fraud cases?

Response	Frequency	Percentage	Member States
NO	23	85.2%	IE, LU, HR, SE, NL, FR, EL, BE, AT, FI, LT, CZ, HU, SK, PL, DE, BG, MT, RO, PT, LV, DK, IT
YES	4	14.8%	SI, ES, CY, EE

Q.1.6 If “YES” to Q.1.5, in which of the following areas did you encounter new difficulties?

Response	Frequency	Percentage	Member States
Providing high quality and complete data in suspected (and established) fraud reporting	4	14.8%	SI, ES, CY, EE
Reporting suspected fraud in a timely manner	3	11.1%	SI, ES, EE
Other (please specify)	2	7.4%	CY, EE
Reporting all cases of suspected fraud	2	7.4%	SI, ES
Technical issues with the reporting system (IMS)	1	3.7%	ES

Following Q1.6, please specify "Other".

Member State	Response
CY	Programs funded directly by EU not under shared management e.g. RRF or Erasmus programs or CEF programs where the initiation of the process may come from EPPO or another MS.
EE	In cases under criminal investigation where the investigation has been initiated by the investigative body on its own initiative, the implementing agency often lacks sufficiently detailed information about the circumstances. As a result, it is not possible to prepare comprehensive reporting.

Member State	Response
	Additionally, reports cannot always be created or notifications made without authorization from the investigative body, as this could hinder a swift and effective investigation.

#### Q.1.7 Have you made significant improvements to the quality of your reporting on suspected fraud cases and irregularities in 2024?

Response	Frequency	Percentage	Member States
NO, it was not necessary	9	33.3%	SE, BE, AT, CZ, DE, MT, EE, LV, DK
YES, we have improved the completeness of the reporting	9	33.3%	FR, EL, SI, ES, PL, BG, RO, PT, IT
YES, we have improved the accuracy of the reporting	7	25.9%	SI, PL, DE, BG, RO, PT, IT
NO, not yet	5	18.5%	HR, NL, LT, ES, CY
YES, we have improved the timeliness of the reporting	5	18.5%	FI, HU, SK, RO, IT
Not applicable	3	11.1%	IE, LU, SI
NO	1	3.7%	DE

#### Q.1.8 What are the main steps you have taken to improve the reporting of irregularities?

Response	Frequency	Percentage	Member States
Enhanced training for staff members	16	59.3%	HR, FR, EL, AT, FI, ES, HU, SK, PL, DE, BG, CY, EE, RO, DK, IT
Improving exchange of information with investigative bodies	12	44.4%	SE, LT, SI, HU, SK, DE, BG, CY, EE, RO, DK, IT
Increase of the collaboration with law enforcement, prosecution services and/or other national authorities	11	40.7%	LT, SI, HU, DE, BG, CY, EE, RO, PT, DK, IT

Response	Frequency	Percentage	Member States
Modifying policies and procedures	11	40.7%	SE, BE, LT, ES, SK, PL, DE, BG, CY, RO, PT
Hiring additional human resources to manage reporting requirements, including data entry and analysis	6	22.2%	LU, HR, BE, SI, MT, RO
Other (please specify)	6	22.2%	IE, HR, NL, CZ, MT, RO
Better technical infrastructures / adoption of new IT tools	5	18.5%	HR, SI, ES, RO, PT
No steps taken to improve the quality of reporting	4	14.8%	IE, AT, ES, LV
Allocation of more resources for system upgrades and maintenance	1	3.7%	RO
More formalised communication channels with EU bodies	1	3.7%	RO

Following Q1.8, please specify "Other".

Member State	Response
IE	There was an ESF+ specific IT system developed, and article 94 simplified cost options were adopted.
HR	AFCOS unit periodically checks press releases of EPPO and State Attorney's Office. If AFCOS unit gets an information that EPPO / State Attorney's Office requested indictment of natural / legal persons in Croatia, it checks whether the case has been reported via IMS and it contacts the competent MCS body to create follow up or initial request.
NL	new coordination anti-fraud expenditure as part of AFCOS to improve the anti-fraud (reporting) process.
CZ	The system mechanisms (methodologies, processes established) have been further developed.
MT	Kindly refer to Questions 1.2 and 1.4.
RO	NAFS (national anti-fraud strategy) – establishment of the irregularity reporting network

Q.1.9 If “NO, not yet” or “NO” to Q.1.7, what are the main reasons preventing you from further improving the quality of reporting in 2024?

Response	Frequency	Percentage	Member States
Insufficient exchange of information with investigative bodies	4	14.8%	HR, LT, ES, CY
Legal or regulatory constraints	4	14.8%	HR, NL, ES, DE
Staff not adequately trained or skilled to manage reporting requirements	4	14.8%	HR, NL, LT, ES
Limited human resources to manage reporting requirements, including data entry and analysis	3	11.1%	HR, ES, DE
Insufficient technical infrastructures	2	7.4%	HR, ES
Other (please specify)	1	3.7%	DE

Following Q1.9, please specify "Other".

Member State	Response
DE	<p>The Federal Ministry of Labour and Social Affairs (BMAS): Currently, no improvements are considered to be required.</p> <p>The Bremen ERDF Managing Authority: The mandatory reporting procedures in place are sufficient. Moreover, as there were no cases of fraud in Bremen, it has not been necessary to improve the quality of reporting.</p>

Q.1.10 In 2024, have you encountered any difficulties in providing timely updates about the follow-up to irregularities, and in particular, fraudulent irregularities?

Response	Frequency	Percentage	Member States
NO	14	51.9%	IE, LU, SE, NL, FR, EL, BE, AT, FI, CZ, DE, MT, LV, IT
YES, only fraudulent irregularities	11	40.7%	HR, LT, SI, HU, SK, PL, BG, EE, RO, PT, DK
YES, all irregularities	2	7.4%	ES, CY

Q.1.11 In which areas did you encounter more difficulties when updating already reported fraudulent irregularities?

Response	Frequency	Percentage	Member States
No difficulties encountered	11	40.7%	IE, LU, FR, BE, AT, FI, CZ, ES, DE, MT, LV
Timeliness of follow-up	10	37.0%	HR, LT, SI, ES, HU, SK, DE, EE, DK, IT
Completeness of information received	8	29.6%	SE, NL, SI, ES, PL, BG, EE, RO
No information received	6	22.2%	HR, ES, DE, CY, EE, RO
Other (please specify)	6	22.2%	HR, EL, BE, ES, DE, PT
Accuracy of information received	3	11.1%	NL, SI, PL

Following Q1.11, please specify "Other".

Member State	Response
HR	Contribution from Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development: Timeliness of information received.
EL	Financial Audit Committee (EDEL): Lack of awareness among and no exchange of information between the judicial authorities and the reporting authorities. Recovery and Resilience Facility Agency (RRFA): To date, no irregularities giving rise to the suspicion of fraud ('fraudulent' irregularities) have been detected.
BE	The exchange of information between judicial and administrative bodies could be streamlined (EFRD, JTF and RRF at the SPW).
ES	Technical difficulties, need to adapt IT systems, which are being improved.
DE	The Rhineland-Palatinate ERDF Managing Authority: Prosecution and judicial proceedings take a long time, and we usually only receive information after actively asking about the case in question.
PT	Follow-up of judicial proceedings

Q.1.12 Regarding previous question, please provide additional explanation about the difficulties encountered.

Member State	Response
IE	n/a
LU	No difficulties encountered.
HR	<p>Contribution from Ministry of Agriculture, Forestry and Fisheries, Directorate of Fisheries: Lack of feedback from investigative bodies on the outcome of the reported case causes difficulties in reporting/follow up of such cases. However, communication and information sharing during the investigations are restricted by law so there is not much space for the improvement.</p> <p>Contribution from AFCOS-unit:</p> <p>Some MCS bodies are not proactive enough in obtaining information needed for reporting updates of already reported fraudulent irregularities. In addition, the flow of information from judicial authorities to reporting authorities is not always prompt.</p> <p>Contribution from Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development:</p> <p>We have encountered difficulties in providing timely updates about the follow-up to fraudulent irregularities due to the length of court proceedings.</p>
SE	In 2024, the Swedish Economic Crime Authority (Swedish AFCOS) found that the managing authorities' investigations relating to reported crimes were legally incomplete, in particular with regard to the nature of the suspected infringement. Therefore, it is difficult to prove that an offence has been committed.
NL	Just setting up the coordination for antifraud, therefor the organisational structure is still in working progress
FR	X
EL	The judicial authorities have not informed the reporting authorities of any notified cases of suspected fraud. Consequently, the reporting authorities cannot update these cases
BE	The exchange of information between judicial and administrative bodies could be streamlined (EFRD, JTF and RRF at the SPW).
AT	No information.
FI	No difficulties encountered
LT	Due to recent personnel changes, we are experiencing a loss of institutional memory, which occasionally hinders our ability to fully update cases or retrieve historical irregularities.
SI	without additional explanation
CZ	N/A
ES	There are many difficulties in getting information from the EPPO and the courts.
HU	The channelling of judicial information could be improved upon



Member State	Response
SK	<p>In individual cases of criminal investigation, access to more detailed information is not possible in order not to interfere with the investigation procedure.</p> <p>Another problem is the length of the criminal investigation process.</p>
PL	<p>In some cases, in which criminal proceedings are still ongoing, it is difficult to obtain up-to-date data from law enforcement authorities due to the confidentiality of proceedings. In particular, this concerns cases where the reporting institution was not the party reporting the criminal offence.</p> <p>Due to the specific nature of criminal cases and the nomenclature used in court judgments, it is sometimes difficult for the reporting institution to establish all personal data of the convicted natural person that must be included in the IMS reporting form. This is because in their judgments, courts do not use the personal identification (PESEL) number, or the registered residence address of the person concerned.</p> <p>A separate category of criminal cases are particularly long criminal/judicial proceedings, the duration of which exceeds the relevant financial perspective.</p>
DE	-
BG	<p>On behalf of the PORB and cooperation with the EPPO office in Bulgaria we could detect some difficulties in obtaining timely and correct information concerning the cases which are already reported to the EPPO, the European Delegated Prosecutors decided not to evoke the case (art.27, par.8 of the Regulation) and therefore they have to be referred without undue delay to the competent national authorities (art.34 of the Regulation).</p> <p>The Ministry of Justice established a procedure in accordance with Art. 24 par. 2 of the Regulation, according to which each prosecutor or investigator, part of the prosecution system (PORB), reports directly to the European Public Prosecutor's Office when a suspicion of an offence within its competence is identified. The centralized channel of communication was overruled which brought to some difficulties and misunderstandings in the process of the exchange of documents.</p> <p>The PORB and especially Department 08 within Supreme Cassation Prosecutor's Office, actively cooperates and assists the EPPO in the process of ensuring prompt, relevant and efficient manner of reporting.</p> <p>The Managing Authorities claimed that receiving a timely information about the measures taken is crucial for the accurate irregularity reporting.</p>
MT	Not applicable.
CY	Bodies initiating cases do not respect the procedure of following up on open cases.
EE	<p>In cases under criminal investigation where the investigation has been initiated by the investigative body on its own initiative, the implementing agency often lacks sufficiently detailed information about the circumstances. As a result, it is not possible to prepare comprehensive reporting. Additionally, reports cannot always be created or notifications made without authorization from the investigative body, as this could hinder a swift and effective investigation.</p>
RO	<p>- Ministry of Development, Public Works and Administration (MDLPA): difficulties regarding the status of the checks undertaken by the other institutions involved. Please note that the judicial authorities have their own investigation deadlines. Please note that in cases where the MA is not party to the process, they do not receive information concerning its finalisation.</p>

Member State	Response
	- AFIR (Agency for the Financing of Rural Investments): Exchange of information – the investigative bodies do not always provide all the information needed to complete the report
PT	The difficulties in obtaining information on the follow-up of judicial proceedings are essentially due to the fact that they are subject to legal confidentiality.
LV	No difficulties encountered.
DK	Regarding timeliness of follow-up, the Danish Business Authority explains that when a suspected case of fraud is reported to the police for further investigation it is not always, that the Managing Authority is noticed of the progress and results of the investigation and decisions made by the police, which makes it difficult to update IMS.

#### Q.1.13 Has the information flow between judicial and reporting authorities improved in 2024?

Response	Frequency	Percentage	Member States
YES, partly	15	55.6%	NL, LT, CZ, ES, SK, PL, DE, BG, MT, EE, RO, PT, LV, DK, IT
NO	10	37.0%	IE, HR, SE, FR, EL, BE, AT, FI, SI, CY
YES, fully	2	7.4%	LU, HU

#### Q.1.14 If “YES, fully” and “YES, partly” to Q.1.13, what steps have been taken in 2024 to improve the exchange of information between judicial and reporting authorities?

Response	Frequency	Percentage	Member States
Establishment of clear instructions for handing over cases and defined guidelines	8	29.6%	LU, CZ, ES, DE, BG, RO, DK, IT
Increased trainings for both judicial and reporting bodies	8	29.6%	ES, HU, SK, DE, BG, MT, RO, IT
Other (please specify)	6	22.2%	PL, DE, RO, PT, LV, DK
Regular inter agency meetings or working groups to discuss ongoing cases and share information	6	22.2%	LT, CZ, ES, BG, RO, IT
No significant changes have been made in 2024	4	14.8%	PL, DE, EE, LV

Response	Frequency	Percentage	Member States
Appointment of liaison officers to facilitate communication and coordination between authorities	3	11.1%	ES, HU, RO
Establishment of formal communication protocols (regular reporting schedules, standardized reporting formats)	3	11.1%	HU, BG, RO
Implementation of a digital platform for real-time sharing of information between authorities	2	7.4%	MT, RO
Setting up of a joint team	1	3.7%	NL

Following Q1.14, please specify "Other".

Member State	Response
PL	In 2024, there was no significant change in the tools used for the exchange of information, while the amount of correspondence between judicial authorities and the reporting institution (queries, replies, clarifications) went up, which also increased the flow of information between entities
DE	The Rhineland-Palatinate ERDF Managing Authority: We (ERDF Managing Authority) are now frequently asking for updates from prosecution officers.
RO	- NAFS (national anti-fraud strategy) – establishment of the irregularity reporting network - AFIR: Every six months, the DCA expert who notified the suspicion of fraud asks the notified authorities about the measures subsequently taken. Protocol of collaboration with the EPPO. Clarification in the control and anti-fraud working procedure on how to notify the EPPO
PT	The information-sharing mechanisms have been consolidated and set in place on support platforms (shared, restricted-access folders updated on the basis of new information in each case).
LV	Cooperation between institutions is constantly promoted and improved.
DK	The Danish Agency for Green Land Conversion and Water Environment: Communication with the judicial authorities has been improved through meetings, clearer instructions when handing over cases and communication about the outcome of cases. Regular follow up with the police regarding the status of the cases.

Q.1.15 Can you provide a short description of the organisational structure and procedures for exchanging information between judicial authorities and reporting authorities in your Member State?

Member State	Response
IE	Where a fraud or suspected fraud is identified, the process to be followed is set out in the various anti-fraud strategies of the managing authority
LU	Organizational structure and procedures for the exchange of information between judicial authorities and reporting authorities detailed in a guideline.
HR	<p>Contribution from Ministry of Finance, Tax Administration: The Tax Administration exchanges information with judicial authorities based on Article 8 of the General Tax Law (no tax secrecy) and the Tax Administration Act. A special Unit - Independent Sector for Financial Investigations was established to cooperate with the EPPO.</p> <p>Contribution from AFCOS unit: Reporting authorities can request AFCOS unit to organize a meeting with State Attorney's Office and the Police (so called AFCOS Network meeting) in order to discuss suspected fraud cases. However, they are encouraged to establish direct communication with judicial authorities in order to speed up the obtaining of information on status of reported suspected fraud and to update the IMS case.</p> <p>Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development have established a special organizational unit for managing irregularities at the level of the Paying Agency responsible for the exchange of information with the judicial authorities.</p>
SE	All cases reported in IMS are sent to the Swedish Economic Crime Authority. If necessary, the prosecutor is contacted to discuss cases. In addition to reporting suspected fraud to the Swedish Economic Crime Authority, information is exchanged at a more general level through the SEFI Council, the national OLAF network (approx. 2 meetings a year), meetings of OLAF's 'Fraud Prevention, Analysis and Reporting' Fraud Prevention Group
NL	There was no coordination for expenditure, in 2024 the AFCOS got this new responsibility, and the organisation is still setting up for better reporting purposes
FR	x
EL	Information is exchanged by email between the judicial authorities and the reporting authorities in order to either provide information or take the appropriate measures to attribute or write off debts.
BE	ERDF, JTF and RRF at the SPW: Exchange of information between the SPW (ERDF, JTF, RRF) and the judicial authorities. The current procedure is as follows: A file is submitted to the Public Prosecutor's Office if there is a suspected irregularity involving a criminal offence. The Public Prosecutor's Office may request additional information concerning the file submitted. Legal basis: Article 29 of the Code of Criminal Procedure - Walloon decrees and/or Walloon government orders specifying the arrangements for communicating information to the authorities depending on the subject concerned. The information exchange procedures have not yet been formally set down in a written procedure
AT	In the event of a notification/message in the IMS, information is requested promptly and provided within a few days.

Member State	Response
	<p>ESF: The procedures and organisational structure for exchanging information are set out and explained in detail in the management and control system of the ESF Managing Authority. The management and control system has been approved by the European Commission.</p>
FI	<p>The authorities responsible for the implementation of EU programmes are administrative authorities, and they exercise administrative powers. Administrative authorities have the power and the obligation, as enshrined in sectoral legislation, to monitor and audit grants and, where necessary, recover them. If administrative authorities have reason to suspect fraud, they make a request to the pre-trial investigation authority, such as the police, for an investigation into the matter. The administrative authorities are also responsible for IMS reporting. The Police or Customs, which have the power to conduct criminal investigations, conduct the preliminary investigation. Following this, the prosecutor issues a decision to bring charges. After that, the matter is dealt with in court. Roles and powers are split among the various authorities. The Police, Customs and the public prosecutors, i.e. the enforcement authorities and judicial authorities, operate independently and have the power to conduct criminal investigations and take coercive measures. Administrative authorities do not have those sorts of powers, but they do communicate the necessary data for the pre-trial investigation authorities to use in connection with a request for an investigation.</p>
LT	<p>The Financial Crime Investigation Service (FCIS), serving as the primary body for reporting and investigating fraud related to EU funds in Lithuania, collects all relevant information from the EU paying agencies in the country and subsequently reports it to OLAF. A key challenge, however, lies in addressing regular irregularities that do not constitute fraud. In such cases, the paying agencies are not obligated to report these instances to the FCIS.</p>
SI	<p>While Ministry for Cohesion and Regional Development answer is YES; The Financial Admin of the Republic of Slovenia answers: NO. Agency for Agricultural Markets explains: Judicial authorities are separate from reporting authorities in organisational terms and work independently. Information is exchanged with judicial authorities in order to meet the needs of administrative procedures. Supreme State Prosecutor's Office of the Republic of Slovenia answers: In our legal system, the police act as the investigating authority, the public prosecutor acts as the prosecuting authority and the court acts as an independent judicial body. In certain cases, particularly more serious offences, the prosecution service may provide guidance to the police during the investigation. Once the investigation is complete, the police submit a criminal report to the prosecutor, together with all the evidence they have collected. The prosecutor then decides whether to initiate criminal proceedings. Our legal system follows the principle of legality, which means that the prosecutor is obliged to initiate criminal proceedings if there is a reasonable suspicion that a criminal offence has been committed and that the perpetrator should be prosecuted ex officio</p>
CZ	<p>The reporting authority is the managing authority of the operational programme. The reporter submits the criminal complaint to the Police of the Czech Republic/EPPO, and it is then dealt with at the Public Prosecutor's Office, and an action is subsequently brought before the court. If the managing authority needs to contact the judicial authorities, the procedure depends on the nature of the particular information. Routine communication (such as the police asking for more detailed information about the project) can also take place directly. Where necessary, other bodies (the certifying authority, the national co-ordination authority, the audit authority) are also included in the communication. In the case of irregularities involving amounts above the established thresholds, AFCOS is also included in the communication.</p>

Member State	Response
	In some OPs, there is a coordinator of audits, controls and irregularities. This staff member communicates with the judicial authorities and the notifying authorities.
ES	The Spanish AFCOS carries out information and monitoring functions for the classification and communication of suspected fraud, informing the authorities of the existence of legal proceedings in progress, as well as their completion, requesting information from the judicial bodies, all on the basis of the criteria contained in the document ‘Classification criteria and procedure for action with regard to irregularities and suspected fraud that are the subject of criminal legal proceedings’ issued by the AFCOS.
HU	The Directorate for Internal Audit and Integrity serves as a single contact point for a two-way flow of information between managing authorities and investigative and judicial bodies, the procedural details of which are laid down in cooperation agreements with the Public Prosecutor’s Office, the police and the National Tax and Customs Administration.
SK	<p>The process of reporting irregularities to OLAF involves several key steps which flows from Managing Authority (MA) or Intermediate Body (IB) through Certifying Authority/Paying Authority (CA/PA) to National Office for OLAF. The MA/IB is responsible for a reporting of detected irregularity and recording the information about irregularity into the national IT monitoring system. For this reason, the MA/IB receives information about any initiated and ongoing procedures from the authorities conducting the procedure.</p> <p>The national monitoring system contains detailed information about the given irregularity, on the basis of which the CA/PA assesses their reporting to National Office for OLAF (AFCOS) and afterwards the National Office for OLAF is reporting the cases to IMS. There is regular communication and exchange of information between all mentioned bodies (for example regarding legal procedures, technical procedures).</p> <p>Other bodies such as the Audit Authority, criminal agency, etc. are involved if necessary. In agricultural funds judicial authorities contact/inform the Agricultural Paying Agency (APA). Then the exchange of information is as follows: APA via IMS to AFCOS. The exchange of information regarding fraudulent irregularities is based on cooperation agreement between AFCOS and the General Prosecutor’s Office of the SR.</p>
PL	The competent institution of the management and control system, after examining a particular case, reports suspected criminal offences to the law enforcement authorities, providing the necessary details substantiating its suspicion. In the area of cohesion policy, where the law enforcement authorities decide to initiate proceedings, further information about the stage of such proceedings is exchanged on the basis of the cooperation agreement between the National Public Prosecutor and the Minister responsible for regional development, which regulates the provision of information on ongoing and concluded proceedings concerning projects co-financed by European funds. On the basis of that agreement, there is a regular, periodic exchange of data on the beneficiaries of EU funds against whom investigative measures have been taken, and some institutions also make use of the possibility to directly contact the designated representatives of the Public Prosecutor’s Office where it is necessary to obtain data on ongoing proceedings without delay. In the area of agriculture, the institution referring a case to law enforcement authorities is obliged to keep the data on criminal proceedings in the relevant register of irregularities up to date until the proceedings come to an end. As a general rule, the exchange of information between the institution and the law enforcement authorities takes place on a regular basis to ensure that the case is kept up to date in the Irregularity Management System. In the absence of information about the current stage

Member State	Response
	<p>of criminal proceedings being conducted by law enforcement authorities, the competent entity must request that such information be sent to the contact point in charge of the respective proceedings, and, on this basis, it must update the data in the register.</p> <p>Information obtained from law enforcement authorities forms the basis for possible reporting or updating of the case in the IMS by the competent reporting institution.</p>
DE	<p>The Federal Ministry of Labour and Social Affairs (BMAS): In the context of the European Social Fund Plus (ESF Plus), there is a guidance document for the ESF Plus Federal Programme which deals with the reporting of irregularities (including suspected cases of fraud). Under the ESF Plus Federal Programme, cases are examined by the managing authority and the intermediate managing bodies. Where necessary, the managing authority instructs the relevant granting authority to take action, which may include, in particular, an on-the-spot check. The granting authority sends an IMS report to OLAF and, where necessary, notifies the offence to the national public prosecutor's office or the European Public Prosecutor's Office.</p> <p>The Federal Ministry of Food and Agriculture (BMEL): Where necessary, cases in the area of agriculture and fisheries are reported to the judicial authorities or the European Public Prosecutor's office by the paying agencies or managing authorities, with the involvement of their legal services.</p> <p>The Bremen ERDF Managing Authority: The intermediate bodies implement operations. Potential cases of fraud are reported to the managing authority while, at the same time, detailed checks are carried out in order to either confirm or dispel the suspicion of possible fraud. If the suspicion of fraud is confirmed, the intermediate body in turn notifies the managing authority and the public prosecutor's office. The public prosecutor's office investigates the case or closes the investigation. The outcome is communicated to the intermediate body, which in turn informs the managing authority.</p> <p>The Baden-Württemberg ERDF Managing Authority: Through Section 2 of the Subsidies Act (SubvG), Germany has obliged (reporting) authorities to disclose facts relevant to subsidies. Under Section 3 of the SubvG, beneficiaries are required to communicate facts which constitute an impediment to subsidies, as well as facts which are relevant to the recovery of subsidies in full or in part. Moreover, Section 6 of the SubvG requires the (reporting) authorities to notify the law enforcement authorities if, in the exercise of their duties, they become aware of facts giving rise to suspicions of subsidy fraud.</p> <p>As a result, a complete chain is established in criminal law between the beneficiary or beneficiaries, the authorities and the law enforcement authorities.</p> <p>The Rhineland-Palatinate ERDF Managing Authority: We formally inform the prosecution officers about any cases as required by German federal law (Section 6 of the SubvG).</p> <p>The Lower Saxony ERDF Managing Authority: In justified cases of suspected fraud, a direct notification (criminal complaint) is made by the intermediate body to the competent public prosecutor's office. The Intermediate body (NBank), investigating authorities and judicial authorities are in regular exchange during the proceedings. The managing authority shall be kept regularly informed of the progress of the procedure.</p> <p>The Schleswig-Holstein ERDF Managing Authority: The MA's guidance document on anti-corruption and anti-fraud measures deals with the handling of suspicious cases and the reporting process. The reporting process is always the same, whichever institution detects a (suspected) case of fraud: If administrative checks confirm a (suspected) case of fraud, a submission is made to the public prosecutor's office via the Electronic Court and Administrative Mailbox (EGVP). An IMS</p>



Member State	Response
	<p>report is also made. The subsequent investigation is the responsibility of the public prosecutor's office.</p> <p>The Thuringia ERDF Managing Authority: Cases where suspicions cannot be dispelled are reported to the law enforcement authorities by the ERDF MA or an intermediate body. If the case is closed, the aforementioned parties are notified. If there are sufficient grounds to believe that an offence has been committed (cf. Section 203 of the Code of Criminal Procedure (StPO)), the law enforcement authorities bring charges.</p>
BG	<p>In the field of penal investigation judicial authorities provide information only in case when Managing Authority is constituted as a victim in the indictment. The Managing Authorities provide assistance to the European prosecutor's Office at requests made for provision of information and documents in order to counteract irregularities and fraud affecting the EU's financial interests.</p> <p>Following the Regulation (EU) 2017/1939 all reporting authorities as well as each prosecutor or investigator, part of the prosecution system (PORB), reports directly to the European Public Prosecutor's Office when a suspicion of an offence within its competence is identified. As a primary point for organizing and ensuring the interaction with EPPO, department 08 within the Supreme Cassation Prosecutor's Office is also reliable link between reporting and judicial authorities and EPPO. The pointed procedures are ongoing practice for years in Bulgaria.</p>
MT	<p>The exchange of information with respect to reported fraudulent cases is established by Article 18 of the Internal Audit and Financial Investigations Act (Cap. 461 of the Laws of Malta).</p>
	<p>For CAPO, they report suspected fraud cases to the relevant authorities (e.g. Police, EPPO, Attorney General- depending on the case), as well as to AFCOS (via IMS and otherwise).</p> <p>AFCOS Organizational Structure:</p> <p>The AFCOS is presided by the Accountant General of the Republic and the following authorities are its members:</p>
CY	<p>(Managing and Control Authorities): Treasury of the Republic of Cyprus, Directorate General for Growth, Ministry of Interior, Cyprus Agricultural Payments Organization.</p> <p>(Legal and Investigation Authorities): Tax Department, Customs and Excise Department.</p> <p>(Prosecution Authorities) Law Office of the Republic, Cyprus Police.</p> <p>(Audit Authorities): The Cyprus Audit Office and the Internal Audit Service are observers. Other relevant authorities which AFCOS has cooperation with is the Independent Authority Against Corruption and the European Delegated Prosecutor (EPPO). Memorandums of Cooperation between the Cyprus AFCOS and other competent authorities involved in the fight against fraud to formalize communication and cooperation forms a deliverable of the TSI project that Cyprus is a beneficiary, and its expected delivery is between August and October of 2025.</p>
EE	<p>The irregularity report is created by the institution responsible for managing of the specific project/beneficiary (implementing agency) in the information system. If the irregularity or fraud is identified by another party (e.g., the Managing Authority, auditing authority, ECA, OLAF, investigative body) or comes from a whistleblower tip, the information is forwarded to the implementing agency responsible for managing of the case. This agency has the legal basis to make financial corrections if necessary or submit a request to the investigative body to initiate a criminal investigation. All irregularities/fraud are recorded to national grant information system from the first euro cent, and the information remains in the system even if it is later determined during the proceedings that no irregularity or fraud has occurred.</p>



Member State	Response
RO	<p>The Managing Authority reports irregularities quarterly via IMS, ensuring that the irregularities have been updated and contain the required information. This includes verifying whether reporting has been initiated for cases they are aware of. Our investigative bodies generally share detailed information only with the institution managing this project. They do not provide separate notifications to the Managing Authority or AFCOS. The Managing Authority obtains the necessary information from the implementing agency or through the reporting system.</p>
	<p>- DLAF: Standardised form in follow-up to DNA/DLAF cases</p>
	<p>- AFIR: In the framework of the Agency for the Financing of Rural Investment, the Control and Anti-Fraud Directorate (DCA) reports directly to the Director-General, who fulfils the duties concerning the role of scrutiny over contracted projects, with a view to the prevention/identification of irregularities and suspected fraud which affect the financial interests of the European Union and the National Budget of Romania. Alongside the control missions carried out on the basis of sanctions and reporting, the Control and Anti-Fraud Directorate ensures ongoing collaboration with bodies responsible for investigating cases of irregularities and (suspected) fraud, representing the main contact point for the AFIR with these institutions. In this regard, the Control and Anti-Fraud Directorate, through the External Operational Cooperation Service, collaborates with OLAF, EPPO, DLAF, DNA, the Police and the Public Prosecution Service on verifying, ascertaining, assessing and monitoring cases of irregularities and suspected fraud. Depending on the information received from the EPPO, DLAF and OLAF, the Control and Anti-Fraud Directorate follows the cases under investigation by the DNA on an ongoing basis, regularly asking about the status of enquiries concerning projects financed by the EAFRD, and of the result of OLAF/EPPO/DLAF/DNA investigations, depending on the way in which the DCA is handling the cases assigned to the Directorate: following the administrative and judicial procedures opened after the discovery of irregularities/fraud, initiating the debt recovery procedure, entering the necessary information in the quarterly report on irregularities, etc. Taking into account the collaboration framework described above, the Control and Anti-Fraud Directorate, through the External Operational Cooperation Service takes over, centralises and analyses the notifications and information received from OLAF, EPPO, DLAF, DNA, the Police and the Public Prosecution Service and cases of suspected fraud opened by other services under the DCA, where necessary ensuring quarterly reporting, monitoring and/or control of cases of irregularity and suspected fraud which have arisen.</p>
	<p>- DGP-AM POPAM: The Managing Authority notifies cases of suspected fraud on the basis of current national legislation, both in writing and through the EPPO website. Information, documents and the outcome of checks/investigations are communicated in electronic and/or paper format depending on each individual case.</p>
	<p>- The Ministry of Energy: Interinstitutional collaboration protocols have been opened in which ways of avoiding irregularities and serious irregularities, such as double financing, fraud or corruption, were identified. - South Muntenia Regional Development Agency (AMPR S–M): establishing official communication protocols, appointing liaison officers in order to facilitate communication and coordination between authorities, regular meetings between agencies or working groups in order to discuss ongoing cases and to exchange information.</p>
	<p>- MIPE – DGPDD: Within the DGPDD – DACNMISC, the Irregularities Officers Department receives requests for information and data from the judicial bodies, responds to requests and regularly requests information on the status of the investigations carried out by the judicial authorities.</p>

Member State	Response
	<p>- MIPE – DGMMRR: Under Procedure No PO. DGMMRR.10- Control of irregularities/double financing, serious irregularities arising in the obtaining and use of external grants and loans allocated to Romania through the PNNR or related national public funds and the recovery of resulting debts. The Audit Control, Recovery and Monitoring Service enters in the register of suspected irregularities/fraud and debtors all cases of suspected irregularities/fraud identified in the checks by the DGMMRR-CN or in findings with financial implications submitted by institutions with responsibilities in this field audit/European Public Prosecutor's Office/DLAF/DNA/OLAF/ANI/DIICOT, etc. Where appropriate, it informs them of the fact that in the course of the checks carried out, a reasonable suspicion arose concerning the identification of evidence of suspected fraud/serious irregularities.</p> <p>- MMAP: Within the framework of the Legal and Debt Recovery Service of the Directorate-General for the National Recovery and Resilience Plan (DGNRR – SJRC), the Department for Controls and the Establishment of Irregularities receives requests for information and data from the judicial bodies, responds to requests and regularly requests information on the status of the investigations carried out by the judicial authorities.</p>
PT	<p>Here, we should point out the information sharing with the Central Criminal Investigation and Prosecution Department (DCIAP) and the European Public Prosecutor's Office (EPPO). The Funds' coordinating bodies are responsible for providing information on operations, beneficiaries, and their respective shareholders/managers/administrators, as well as service providers/suppliers. In turn, the DCIAP and the EPPO provide information on the state of play of proceedings initiated.</p> <p>The Funds' coordinating bodies compile and validate data on irregularities to be reported to OLAF and monitor cases reported to the Public Prosecutor's Office (suspected fraud cases) or to the relevant Operational Programmes, with a view to characterising beneficiaries in terms of good standing, so as to prevent their renewed involvement in similar situations. The information is sent to the AFCOS, which validates it and submits it to OLAF via the IMS.</p>
LV	<p>If, while administering EU funds (instruments or other programmes), a possible illegal act is detected or an act that does not comply with the conditions for implementing EU funds and raises suspicions of fraud that may affect the financial interests of the EU, this act is reported to the European Delegated Prosecutor's Office in Latvia and the European Public Prosecutor's Office (EPPO). The law enforcement authorities can also be contacted - the State Police, the Corruption Prevention and Combating Office - to receive the necessary advice, while at the same time informing the European Delegated Prosecutor's Office in Latvia.</p> <p>The exchange of information between institutions is determined in the AFCOS procedure "Methodological material on cooperation and exchange of information between the Anti-Fraud Coordination Service of the Ministry of Finance (AFCOS), national institutions and the European Anti-Fraud Office (OLAF) in the field of protection of the financial interests of the European Union" and AFCOS procedure "Procedure for institutions to report to the European Public Prosecutor's Office (EPPO) on suspected fraud against the EU's financial interests". Each EU funds administering institution has a contact person for communication with the investigative authorities, and on the side of the investigative authorities there is a contact person for communication with the EU funds institution.</p>
DK	<p>The Danish Business Authority: When we, as a managing authority, find a case, where we after investigations have a reasonable certainty, that we have a case of fraud on our hands, we make a report to the police, who conducts further investigations and decides if it is a case suitable to take to court. We rarely communicate with the police regarding reported cases and almost never with the</p>

Member State	Response
	<p>judicial authorities. When that is said it is also important to underline, that we have very few cases of fraud.</p> <p>The Danish Agency for Green Land Conversion and Water Environment: A special department of the reporting authority designated to handle fraud is in charge of the communication with the judicial authorities.</p>
IT	<p>As stated in the aforementioned ‘Guidelines on how to notify the European Commission of irregularities and fraud against the EU budget’ issued in 2024, all managing authorities have been reminded to always bear in mind that, in the event of difficulties in dialogue with the judicial authorities, they can contact the Guardia di Finanza Unit for Combating Fraud against the European Union at the Prime Minister’s Office, which will seek to facilitate contact with the local branch of the body concerned.</p> <p>In addition, by Order No 6 of 6 December 2024, the Prosecutor General at the Court of Auditors confirmed that at least one staff member authorised to access the IMS platform would be designated at each local public prosecutor’s office.</p> <p>In order to allow the data in the database to be updated in a timely manner, the regional public prosecutor’s offices have been asked to share information with managing authorities on summonses, case dismissals and judgments regarding fraud against the EU budget, with the public prosecutor’s offices at the courts of appeal and Court of Cassation being subject to a similar requirement to share information on judgments issued in appeals.</p>

#### Q1.16 What methods are used for exchanging information between judicial and reporting authorities?

Response	Frequency	Percentage	Member States
Other (please specify)	24	88.9%	IE, LU, HR, SE, NL, FR, EL, BE, AT, FI, SI, HU, SK, PL, DE, BG, MT, CY, EE, RO, PT, LV, DK, IT
Standardised digital forms	11	40.7%	LU, HR, SE, BE, LT, CZ, ES, DE, BG, EE, RO
Secured online platforms	6	22.2%	SI, CZ, DE, MT, RO, IT
Regular meetings	5	18.5%	HR, CZ, SK, BG, RO
IMS	4	14.8%	AT, CZ, ES, DE
Shared case management system for tracking and reporting suspected fraud case	3	11.1%	CZ, ES, RO

Response	Frequency	Percentage	Member States
Automated data exchange systems	2	7.4%	ES, EE

Following Q1.16, please specify "Other".

Member State	Response
IE	?
LU	In addition to response to Q.1.15., conventional communication methods (e.g., email, written correspondence, telephone calls, etc.) are equally used.
HR	Contribution from AFCOS unit: Formal written communication. Contribution from Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development: Inquiries sent by post or email.
SE	The Swedish Economic Crime Authority is notified quarterly of any reported cases. Following discussions with the Swedish Economic Crime Authority, information is shared in the most appropriate way. It can be done by encrypted email, by letter or on a USB stick. The Swedish Economic Crime Authority's website has digital forms for reporting crimes and filling in other relevant information. There are also links to tip-off functions and to the Swedish Economic Crime Authority's whistle-blower channel for reporting wrongdoing involving the Union's financial interests in Sweden.
NL	At this moment the AFCOS is trying to get IMS authorisation for a better insight of the irregularities
FR	For the CAP - The exchange of information takes place between the judicial authorities and the paying agencies. These exchanges are then forwarded to the Secretariat of the CICC EAGF, which is responsible for officially submitting fraudulent and non-fraudulent data to OLAF. Equally, for the NRRP - In January 2024, an agreement was signed by the MICAF, the Treasury DG and the European Public Prosecutor's Office (EPPO) on operational cooperation on the reporting of offences in the context of the national recovery and resilience plan (NRRP) that fall within the competence of the EPPO. This working arrangement will act as a framework for enhanced cooperation between the EPPO and the French authorities in charge of administrating this funding. A form for reporting fraud to the EPPO in France and a practical manual were annexed to the working arrangement.
EL	Any information from the judicial authorities is sent by letter and/or by email.
BE	Via email
AT	Direct communication – as befits the particular situation - is conducted by email with the Authorising Body and/or the Paying Agency. ESF: By means of electronic files (ELAK).
FI	A request for an investigation is made in a standard format, and a digital form or other form of notification can be used.

Member State	Response
SI	AAMRD answers: Communication in writing by means of correspondence, which is recorded in the Agency's document database. Supreme State Prosecutor's Office of the Republic of Slovenia answers: Information exchange between judicial and reporting authorities is primarily based on document-based communication. Although a limited form of electronic exchange has been established between police, prosecutors' offices and courts, the operational processes are still predominantly based on the exchange of physical documents. This traditional approach ensures compliance with procedural and legal requirements. Efforts are underway to improve electronic data exchange and streamline communication, but full digitisation has not yet been achieved
HU	The information exchange process set out in cooperation agreements.
SK	Documentations and information received in accordance with Cooperation agreement and law obligation.
PL	<p>A regular exchange of information on the basis of the cooperation agreement between the National Public Prosecutor and the Minister responsible for regional development, as regards the transmission of information on ongoing and concluded proceedings concerning projects co-financed by European funds:</p> <ul style="list-style-type: none"> <li>- periodic cooperation – receiving from the National Public Prosecutor's Office information on proceedings in cases in which the public prosecutor handling the case has consented to the transmission of information regarding those proceedings to the institution;</li> <li>- ongoing cooperation – exchange of information via a dedicated e-mail address where it is necessary to obtain data on specific proceedings;</li> <li>- direct referral of questions by managing authorities to individual public prosecutors' offices regarding specific ongoing proceedings.</li> </ul> <p>- The exchange of information at the stage of judicial proceedings is a formal process governed by the relevant legislation. In addition, the competent national institutions have access to digitised casefiles and to a judicial information portal, which facilitates communication and exchange of information between the judicial authorities and these institutions. However, the decision on whether or not to grant access to casefiles (including in digital form) is taken, in accordance with the relevant legislation, by the authority handling the case.</p>
DE	<p>The Federal Ministry of Labour and Social Affairs (BMAS): In the context of the ESF Plus Funding Programme, ESF managing authorities report suspected cases of fraud to OLAF via the IMS system. The judicial authorities (public prosecutor's offices) are informed in writing of suspected cases of fraud, outside of the IMS.</p> <p>The Federal Ministry of Food and Agriculture (BMEL): Parallel transmission of the relevant case files.</p> <p>The Rhineland-Palatinate ERDF Managing Authority: Report via letters (on paper).</p> <p>The Lower Saxony ERDF Managing Authority: In the case of a criminal complaint, an official letter from intermediate body (NBank) is sent to the public prosecutor's office. There is no regular exchange.</p> <p>The Saarland ESF Managing Authority: Forwarding to the internal legal department.</p> <p>The Thuringia ERDF Managing Authority: Email, letter, telephone.</p>

Member State	Response
BG	Written reports and correspondence. Receiving judicial follow-ups, when the Managing Authorities are constituted as a party in trial.
MT	In cases reported as fraudulent by IAID, the information is forwarded to judicial authorities by hand. (registered as private and confidential).
CY	Confidential correspondence (Email and Letter Communication)
EE	Meetings and information exchange regarding fraud suspicions.
RO	<ul style="list-style-type: none"> <li>- DLAF: standardised form (legal follow-up)</li> <li>- DGP-AM POPAM: written correspondence</li> <li>- MIPE – DGPDD: The transmission of requests in digital form and the communication of responses in digital/paper form, depending on the situation.</li> <li>- MIPE – DGMMRR: to the European Commission audit services (DG EC-FIN) and ECA secure online platforms. To the judicial authorities in letters and supporting documents.</li> </ul>
PT	Information is shared by means of restricted email and joint recording in secure-access folders reserved for the parties involved in the proceedings.
LV	Official correspondence, electronic correspondence, telephone communication.
DK	<p>The Danish Business Authority: The occasional phone call or e-mail.</p> <p>The Danish Agricultural and Fisheries Agency: Secure tunnel mail system.</p> <p>The Danish Agency for Green Land Conversion and Water Environment: The specialised department of the reporting authority sends a report to the police via secure digital mail and any communication between the authorities is by secure digital mail.</p>
IT	<p>Judicial authorities and reporting authorities (MAs) exchange information through formal data update requests. The reporting authority sends such a request directly to the judicial authority or, if the IMS report originated from a notification received from an external control body (e.g. a police force), sends it via that body. In the latter case, on each occasion the body concerned will request the necessary prior approval from the judicial authority that is conducting the investigation.</p> <p>See the information given in response to Q.1.4 and Q.1.5 for cases where problems or difficulties arise in the flow of information.</p> <p>In the context of the activities aimed at fighting fraud against the European budget, the control bodies in general (with specific reference to the police forces) draft a summary report upon completion of their inspection activities, in parallel with the notifications of findings that are sent to the competent criminal-law and accounting-law judicial authorities to allow them to move forward with their proceedings. They send this report by email to the Office of the Prosecutor General at the Court of Auditors for statistical analysis, for coordination with the local public prosecutor's offices and possibly so that action can be taken.</p>

Q1.17 Do you see possible improvement in the exchange of information between judicial and reporting authorities? If yes, which ones? How can OLAF / the Commission support this?

Member State	Response
IE	AFCOS are working with the relevant MAs to ensure the process is clear to all parties.
LU	No need for improvement identified.
HR	<p>Ministry of Regional Development and EU funds - Directorate for the Implementation of the Operational Programmes and Financial Instruments propose that OLAF regularly informs Member States about the start and end of investigations it conducts.</p> <p>Contribution from Ministry of Finance, Tax Administration: Conclusion of a working agreement with EPPO and enabling EPPO to have direct access to certain databases of the Tax Administration.</p> <p>Contribution from AFCOS unit: The exchange of information between judicial and reporting authorities could be improved by mutual trainings (MCS bodies could be trained in the area of Criminal Act, Criminal Proceedings Act and practice of judicial and investigative bodies while judicial and investigative bodies could be trained in the area of management and control of EU funds). OLAF could contribute as an organizer of targeted training activities or a speaker at training activities organized by Croatian authorities. In addition, a round table could be organized in order to discuss difficulties related to handling suspected fraud cases from the aspect of MCS bodies and judicial bodies.</p> <p>Contribution from Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development: The exchange of information can be improved by using standardized digital forms between judicial and reporting authorities.</p>
SE	Training of case handlers working for the managing authorities, and enabling the authorities to strengthen their internal processes, including justifying why an identified regularity is not considered a suspected crime
NL	The new responsibility takes time to get the organisational structure in place, at this moment no help is needed from OLAF/Commission
FR	x
EL	The exchange of information between judicial and reporting authorities could be improved through the development of an automated data exchange platform (to which all parties involved would have access).
BE	ERDF, JTF and RRF at the SPW: Yes, work is under way to formally set down an information exchange procedure between the judicial authorities and the reporting authority. The purpose of this is not only to improve cooperation and the regular exchange of information but also to standardise the procedural practices for the submission of files reporting suspected infringements involving a criminal offence. OLAF can support the creation of these procedures by providing information on the information exchange procedure between the judicial authorities and OLAF and also by giving



Member State	Response
	examples of the file submission and information exchange procedure in other Member States or the standard procedures expected by OLAF.
AT	No, support from OLAF is not necessary.
FI	This is a national competence, and the Commission has no role to play in it.
LT	Automated data exchange systems or IMS can be used for internal information exchange
SI	<p>Supreme State Prosecutor's Office of the Republic of Slovenia answers: Yes, there is room for improvement in the exchange of information between judicial and reporting authorities. Key areas for improvement include:</p> <ul style="list-style-type: none"> <li>- Automated transfer of attachments from police to prosecution registers - This would reduce administrative workload and minimise manual data entry and document scanning. A pilot test has started but has been delayed due to technical constraints. The plan is to gradually extend the test to other regions if the technical feasibility is confirmed.</li> <li>- Electronic filing of court documents - Intensive discussions have taken place with the courts to initiate its use and the necessary system upgrades are being tested. The first phase of testing will start early in 2025 and will focus on lower court cases. OLAF and the Commission could assist by facilitating technical solutions, promoting interoperability standards and providing funding or expertise for digital transformation projects. Promoting cross-border best practices and ensuring alignment with EU-wide digital justice initiatives would also be beneficial.</li> </ul>
CZ	Cooperation is at a very high level. No calls for improvements have been received.
ES	<p>An improvement would be to be able to obtain more information from the EPPO and for it to be communicated to AFCOS in a systematic way, at least annually, with basic information within the limits allowed by the regulations of:</p> <ul style="list-style-type: none"> <li>- cases that have been transferred to the National Court, cases that have been finalised in the EPPO, and, cases where there is an ongoing investigation in the EPPO. OLAF could help by establishing general rules.</li> </ul>
HU	It could be improved by continuing the ongoing development of internal cooperation between Member States' bodies. OLAF can support such processes by comparing and disseminating existing national practices.
SK	More trainings to strengthen the prevention and detection of fraud and irregularities, creating new secure online platform.
PL	<p>Yes, with regard to some aspects of cooperation, we saw opportunities to improve the exchange of information between the judicial authorities and the reporting bodies. For example, preparatory work is currently underway at the Institution Coordinating the Partnership Agreement in connection with the conclusion of an agreement with the National Public Prosecutor, which covers information on draft cohesion policy programmes under the 2021-2027 financial perspective. The objective of the agreement is to define new rules of cooperation and the methods and means of exchanging information.</p> <p>The Paying Agency's cooperation with law enforcement authorities consists in providing all the information these authorities require for their investigations in its entirety and in a timely manner.</p>



Member State	Response
	Professional representatives of the institutions, both at the stage of preparatory proceedings and, potentially, at the stage of judicial proceedings, carry out all the procedural steps provided for by law and submit requests to the law enforcement authorities for access to information concerning the stage of the relevant proceedings. However, it is for law enforcement authorities and courts to take any decisions regarding the scope of information on ongoing proceedings to be provided and on the manner of providing it. At the same time, new solutions, such as the above-mentioned digitalisation of casefiles and the judicial information portal, have greatly facilitated the institutions' process of obtaining information about ongoing proceedings. However, the decision on whether or not to grant access to casefiles (including in digital form) is taken, in accordance with the relevant legislation, by the authority handling the case.
DE	<p>The Baden-Württemberg ERDF Managing Authority: No, there is currently no need to improve the exchange of information between judicial and reporting authorities.</p> <p>The Bremen ERDF Managing Authority: No, the existing possibilities for exchanging information are sufficient.</p> <p>The Thuringia ERDF Managing Authority: Faster processing by OLAF; definition of vague legal concepts; updated manual/guidance on irregularities; recommendations for action; presentation of 'best practice' procedures.</p>
BG	Through specialized targeted trainings and awareness-raising tools (online materials) for specialized units in the structure of the reporting authorities. Strengthening and increasing the level of cooperation with the Prosecutor's Office of the Republic of Bulgaria. Updating the cooperation agreement between OLAF and Prosecutor's Office of the Republic of Bulgaria. Amendments in criminal procedural legislation are needed. An improvement in the exchange of information between judicial and reporting authorities can be achieved through informing the reporting authorities of the results of judicial proceedings/sending final judicial decisions. Start using digital platforms, like automated data exchange systems.
MT	Yes, receiving periodical feedback from judicial national authorities and the EPPO.
CY	Yes, establishment of an online secured platform via which all the national authorities (AFCOS members and Judicial Bodies e.g. Attorney General/EPPO /Independent Authority Against Corruption/Police can exchange information on reporting and also on status of cases.
EE	We exchange general information on a regular basis, but it is not possible to share detailed information on specific cases. This is regulated at the national legal level.
RO	<p>- DLAF: Yes. The communication of specific information on the reporting criteria in the IMS. Specific regulations concerning reporting by the judicial authorities.</p> <p>- AFIR: Yes. Following criminal investigations, insofar as irregularities in the use of EU funds are found, the competent bodies could send evidence to the AFIR with a view to triggering the procedures for detecting irregularities and establishing budget debts independently of the outcome of criminal investigations. The organisation of the training session on reporting.</p> <p>- DGP-AM POPAM: Yes, through the conclusion of protocols between the judicial and reporting authorities for the quarterly matching of cases referred for investigation. We think that the Commission could regulate this type of activity.</p>

Member State	Response
	<p>- The Ministry of Energy: By providing regular information at courses or seminars specifying methods for avoiding the risk of fraud and corruption arising from relevant cases or from allowing access to databases or reports generated from them for companies considered to be ineligible and to be avoided.</p> <p>- West Regional Development Agency (ADR VEST): The exchange of information between the judicial and reporting authorities can be improved by the adoption of mechanisms and procedures. Possible measures include: the conclusion of agreements/protocols between the judicial and reporting authorities. The organisation of joint training sessions: these could improve mutual understanding of the needs and responsibilities of each party involved. The development of automated systems for the supply of/access to data/information – interoperability of databases. - MIPE – DGPDD: Through the creation of an automated data exchange system</p> <p>- MIPE – AM POCU: Yes, through the implementation of a digital platform for the exchange of information in real time between authorities</p> <p>- MIPE – DGPS: Yes, through the organisation of regular meetings or through the creation of an automated data exchange system.</p> <p>- MIPE - DGMMRR: The judicial authorities have access to the platforms used in the management/implementation of the PNRR. In this respect, collaboration protocols have been concluded between MIPE -DGMMR and institutions with investigative/control tasks.</p> <p>- MIPE - Directorate-General for Just Transition and Economic Competitiveness (DGTJCE): there is a common DLAF/DNA/EPPO database</p> <p>- MMAP: Through the creation of an automated data exchange system</p>
PT	Yes, through the creation of dedicated IT platforms to be used jointly by judicial bodies and administrative authorities, in order to enable up-to-date monitoring of cases and faster information sharing.
LV	Develop more secure and specialized information exchange channels. Financial support for developing digital tools.
DK	No possible improvement reported.
IT	The European Public Prosecutor's Office (EPPO) established by Regulation (EU) 2017/1939 has been fully operational for around three years and is competent for almost all types of crime against the financial interests of the EU. We thus believe that there should be a more robust form of information sharing between OLAF and the EPPO, including as regards the possible introduction of a single fraud detection and monitoring system. OLAF could support this process as part of its relations with the EPPO.

**Q.1.18** Please feel free to share any additional thoughts or experiences you have regarding the topics discussed in this section.

Member State	Response
IE	n/a

Member State	Response
LU	N/A
HR	<p>Contribution from AFCOS unit:</p> <p>In October 2023 OLAF organised an online training for Croatian authorities that was attended by more than 300 participants. In addition, in October 2024 OLAF organised a webinar on IMS refactoring. Croatian authorities found the trainings very informative. However, they expressed need for more specific trainings that would include case studies and exchange of practice with OLAF and member states as well as periodical trainings on the use of IMS where reporting challenges could be presented and discussed.</p>
SE	N/A
NL	N/A
FR	x
EL	No further comments required.
BE	/
AT	No information.
FI	-
LT	-
SI	-
CZ	-
ES	Possibly one way to get authorities to report irregularities to OLAF completely, correctly and on time would be to establish some kind of consequence for non-compliance depending on the seriousness of the non-compliance and applying the principle of proportionality.
HU	The establishment of a single contact point (Directorate for Internal Control and Integrity) has, on the basis of experience so far, already added significant value in its cooperation with investigative and judicial bodies.
SK	x
PL	None
DE	<p>The Lower Saxony ERDF Managing Authority: The exchange between the authorities and intermediate body (NBank) in case of a criminal complaint via the direct communication channels and the close exchange is guaranteed at all times.</p> <p>Bremen: There were no potential cases of fraud in 2024.</p>
BG	N/A
MT	Kindly refer to the replies provided.

Member State	Response
CY	No additional thoughts.
EE	If possible, the EPPO regulation could stipulate the exchange of information on investigations and cooperation with AFCOS's.
RO	The Ministry of Energy: We consider that access to interconnected databases in which to check financial and legality aspects in order to exclude companies which are not eligible would help to mitigate possible irregularities.
PT	<p>The purpose of establishing a body of facts preventing and restricting access to the EU Funds is to prevent and combat fraudulent practices in connection with receiving financing from the Funds, based on rigorous scrutiny of applicants. This is achieved through the creation, management and consultation of a database containing relevant information on the good standing and debt situation of parties that have already benefited or will benefit from support from the EU Funds. The European Commission's growing concerns about fraud and the establishment of channels for the handling of complaints/reports on the use of support co-financed by the Cohesion Policy Funds have made it necessary to adopt a specific methodology for determining parties' good standing and debt situations, which enables this access requirement to be managed effectively. This should be instrumental in assessing the level of risk that parties may present, thereby making a decisive contribution to the effective protection of the financial interests of the EU and of the Member States, based on the coordination of various sources of information found in databases held by national authorities and made available by the European Commission.</p> <p>For Portugal 2030, the codification regarding good standing, reliability and debt situation to be observed in the classification of parties receiving or applying for support from the Cohesion Policy Funds has been approved, as has the procedure for managing this information. In other words, the information on the good standing, reliability and debt situation of beneficiaries of the EU Funds must be kept in a specific information system, which supports the action of all the bodies involved in Portugal 2030, and determines the subsequent action of the managing, paying and auditing authorities in respect of applications or projects of beneficiaries that have already been approved. The codification of this information was based on data contained in audit/monitoring reports, complaints, criminal or administrative proceedings for violations of legislation on child labour and discrimination in work and employment, enforced collection proceedings through the tax courts (tax enforcement proceedings), insolvency proceedings and special revitalisation proceedings.</p>
LV	NA
DK	<p>The Danish Agency for Green Land Conversion and Water Environment: Denmark reports cases of suspected fraud to the Commission when such a case is handed over to the police. A police investigation can be time-consuming, and it is natural that it will occasionally disprove the suspicion. Those conditions contribute to the observed trends with cases being open for a long time and cases that do not lead to prosecution. Nevertheless, there is still a potential for improvement in the area and the paying agency for agricultural support has implemented a significant effort to achieve in the period 2022-2024.</p> <p>The Agency has set up a unit to follow up on cases of suspected fraud or circumvention in order to secure resources and the right skills for the task. This has significantly reduced case processing time and improved the quality of police reports in the paying agency, which provides better conditions for the police to follow up on the reports. Since the end of 2023, the case processing time at the police has also gradually decreased with</p>

Member State	Response
	regard to reports of suspected subsidy fraud. The paying agency held a meeting with the Director of Public Prosecutions in February 2024. The meeting has improved cooperation between the authorities through a better common understanding of the legal basis. In the second half of 2024, the paying agency has noted an increase in the number of reports coming before a court. The Paying Agency for Agricultural Support will maintain the cooperation and internal efforts with the expectation of achieving further improvements in the area.

**Q.2.1. Have you ensured that the digitalisation of the fight against fraud is part of your NAFS (National anti-fraud strategy)?**

Response	Frequency	Percentage	Member States
YES	10	37.0%	FR, AT, ES, HU, SK, MT, RO, PT, LV, IT
Not yet, but we intend / are in the process of developing this part of the strategy	8	29.6%	LU, NL, BE, FI, LT, CZ, BG, CY
Digitalisation of the fight against fraud is part of another strategy / assessment / policy (please specify)	7	25.9%	HR, SE, EL, SI, PL, EE, DK
NO	2	7.4%	IE, DE

**Following Q.2.1, please specify "Digitalisation of the fight against fraud is part of another strategy / assessment / policy".**

Member State	Response
HR	<p>The Republic of Croatia has adopted two anti-fraud strategies related to the protection of the EU's financial interests so far and they were both communicated to OLAF. One covered the period 2010-2012 (adopted 14/01/2010) while the other covered the period 2014-2016 (adopted 23/01/2014), and both strategies were fully implemented. Considering that the Anti-Fraud Coordination System in the Republic of Croatia has been established, fully operational, and no major weaknesses were identified, there were no new anti-fraud strategies aimed at protection of financial interests of the EU adopted, neither update of the existing ones have been made. Yet, AFCOS system in the Republic of Croatia has been constantly fine-tuned through softer measures. Contribution from the Ministry of Finance, Custom Administration: In Implementation Programme of the Ministry of Finance</p> <p>(<a href="https://mfin.gov.hr/UserDocsImages/dokumenti/proracun/stratesko/Provedbeni%20program%20Ministarstva%20financija%20za%20razdoblje%202025.-2028.pdf">https://mfin.gov.hr/UserDocsImages/dokumenti/proracun/stratesko/Provedbeni%20program%20Ministarstva%20financija%20za%20razdoblje%202025.-2028.pdf</a>) – Measure 29 prescribes "Enhancement of digitalisation and adjustment of e-customs, excise and other information systems and optimization of infrastructure and equipment.</p> <p>In addition, Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture</p>

Member State	Response
	and Rural Development and Directorate of Fisheries highlighted the following answer: Not yet, but we intend / are in the process of developing this part of the strategy.
SE	Implementing authorities, AFCOS and audit body all have different digitalisation strategies and policies.
EL	Digitalisation concerns the sectoral Anti-Fraud Strategy (Structural Funds) of the programmes under the 2021-2027 Partnership Agreement for Regional Development (ESPA). In particular with regard to the reception and examination of complaints concerning the programmes/projects co-financed under the 2021-2027 Partnership Agreement for Regional Development, Article 50(1) of Law 4914/2022 states that ‘The Secretariat-General for Public Investments and the Partnership Agreement for Regional Development (ESPA) of the Ministry of Development and Investment, through the Special Service for Institutional Support and Information Systems (EYTHYPS), is responsible for ensuring that complaints which fall within the scope of the programme are examined by means of the management and control system(s). In order to simplify and accelerate the procedure between the stakeholders, complaints and examination findings are recorded, information is exchanged, and the related documents are transmitted electronically by authorised users, through the integrated information system (IIS).’ Implementation of the above-mentioned provision in the IIS is expected to start later this year. The MAs, responsible for detecting irregularities in co-financed projects, exchange relevant information using the authorised access of the Anti-Fraud Officer in each MA to the special space created for the Internal Anti-Fraud Network on the DIAVLOS electronic platform. The technical infrastructure of the IIS has been set up to allow it to interconnect with the central beneficial ownership register. The pilot operation phase has been completed and full operation is expected in the immediate future. The NTA/AFCOS networking platform is used by AFCOS and the competent ESPA authorities to facilitate the management and best possible identification of complaints submitted concerning co-financed projects and operations. Cooperation through this tool is always encrypted using strong authentication procedures for accredited users only.
SI	Financial Amin. of the Republic of Slovenia: Indeed, the digitalisation is the part of the Strategy of the Financial Administration of the Republic of Slovenia (FARS), FARS Work Program and the FARS Annual Report. Furthermore, the risk management, risk analysis and Compliance Risk Management (CRM) are also included in such strategy for particular working fields.
PL	Poland has not adopted a national anti-fraud strategy (NAFS). Poland has not decided to create such a document, and the European Commission does not oblige Member States to do so. The competent institution of the management and control system, on the other hand, have mechanisms under which they carry out their anti-fraud mission, including the digitalisation of anti-fraud measures. The managing authorities of all cohesion policy programmes are required to draw up a document on how to prevent and deal with corruption and fraud, including conflicts of interest within the respective programme. The authorities also include information on the digitalisation of anti-fraud measures in their documents. This programme-based approach allows for a proper assessment of the current situation with regard to anti-fraud measures, and for risk assessment and the development and introduction of proportionate measures to combat fraud at the lowest possible management level. When drawing up programme documents, the institutions involved in the implementation of EU funds also take account of the fact that fraudulent operators use new technologies to commit fraud. To counter this, growth concepts are being developed for the existing IT tools and ways in which

Member State	Response
	they can be used to combat fraud. In this way, the digitalisation of the area of implementation, management and control of cohesion policy is constantly evolving (implementing new functionalities and improving existing functionalities), and it is at a rather advanced stage in Poland. There are direct possibilities for the digitalisation of the fight against fraud and the use of modern technologies in Poland by the relevant investigation services.
EE	<p>Estonia's digitalization strategy can be called the "Digital Society Development Plan 2030" (DAK), and to implement it, each ministry prepares an ICT strategy for its own field. The DAK does not contain sectoral digitalization goals, and these should be included in the ICT strategy of the MoF, which is not a public document.</p> <p>We do not have a NAFS at the national level. We have several different strategies, and all these documents have digitalisation information. We have established minimum requirements for controls, created a cross-check possibility between different databases. Additionally, we have proposed cooperation with national investigative bodies, which could contribute even more to the analysis of digital data related to grants to identify potential vulnerabilities and fraud. Once agreements are reached, they can also be formalized or confirmed at the level of a strategy, cooperation agreement, or other document.</p>
DK	Digitalisation of the fight against fraud is part of the anti-fraud strategy of EMFF/EMFAF in Denmark.

**Q.2.2. If “YES” to Q.2.1, please describe how it has been implemented.**

Member State	Response
FR	<p>In combating revenue fraud, for example, the French customs administration plans to make use of data mining in order to establish rapidly the profiles of at-risk traders. On the expenditure side, the DGEFP has developed a complete data science platform making it possible to identify risk elements in the files and, thereby help the departments managing the ESF to detect fraud.</p> <p>France's NAFS has promoted regular use of the Early Detection and Exclusion System (EDES) to various authorities.</p>
AT	Use of the ARACHNE data mining tool
ES	The NAFS includes measures such as the improvement of tools for risk analysis, the widespread use of databases for prevention and detection purposes, and the analysis of the interoperability of databases. On the other hand, the guidelines of the State Tax Agency's tax and customs control plan focus on the use of technology in the fight against fraud.
HU	On the basis of the periodic review of the EUPR and FAIR system with a view to exploring and taking advantage of opportunities to prevent fraud and corruption, improvements have been made to the fraud prevention function, to manage project transfers and succession, strengthen the link with the Irregularity Management Database and enable ARACHNE commitments to be implemented.



Member State	Response
SK	<p>The Slovak Republic aims to ensure that the digitalization of the fight against fraud is an integral part of our National Anti-Fraud Strategy (NAFS). This strategy emphasizes the need to utilize all available IT tools (including ARACHNE) in the fight against fraud and calls on the relevant authorities to use these tools in their activities for the prevention and detection of fraud cases and other irregularities. The structured exchange of data and information between anti-fraud authorities and managing authorities is highlighted in the NAFS as a fundamental principle of fraud investigation and prosecution.</p>
MT	<p>A Central Document Repository System (CDRS) has been implemented through the creation of a digital platform that allows file and document sharing between 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) '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'.</p> <p>The CDRS was set up in line with Action Points 13 and 14 of the National Anti-Fraud and Corruption Strategy (NAFCS), as well as Malta's Recovery and Resilience Plan (RRP) commitments, and has the following features:</p> <ul style="list-style-type: none"> <li>- Stores electronic documents;</li> <li>- Offers a centralised access to documents that can be easily retrieved by the members of the Co-ordinating Committee; and</li> <li>- Provides the necessary security for sensitive information.</li> </ul> <p>In addition, IAID has compiled a list of software tools that are being used to assist each member of the Co-ordinating Committee in the prevention, detection, reporting, investigation, prosecution and correction of fraud and corruption irregularities.</p> <p>Information provided regarding (1) the procurement method used and (2) the involvement of the Ministries' respective Information Management Unit (IMU) in the procurement of new software restricts procurement duplications and also ensures that the use of such software is optimized, as well as enables the sharing of best practices in the use of software tools.</p>
RO	<ul style="list-style-type: none"> <li>- ADR VEST: Specific objective No 1.4. Streamlining the reporting of irregularities within the framework of the 2023-2027 NAFS aims to standardise and create a uniform reporting process, and ensure the quality and comparability of the data provided by the Romanian authorities, bearing in mind the need for the European Commission to set up a uniform digital, interoperable system for the collection of comparable data on irregularities and cases of fraud from the EU Member States.</li> <li>- AFIR: The existence of the Register for Suspected Fraud and Indicators of Fraud and of the Electronic Register of Evidence of AFIR correspondence with EPPO, DNA, DLAF, IPJ, OLAF, DG Agri, and ECA: both registers are managed by the External Operational Cooperation Service of the Control and Anti-Fraud Directorate. In the Register for Suspected Fraud and Indicators of Fraud, the irregularities officer, a position provided for by Article 25 of Government Decision No 875/2011 approving the implementing rules for Government Emergency Order No 66/2011, keeps a record of the referrals to the EPPO/DNA, DLAF pursuant to Article 8(1) or (11) of Government Emergency Order No 66/2011 concerning projects relating to the 2007-2013 and 2014-2020 NRDPs and the transition period in which suspected fraud or attempted fraud has been identified.</li> </ul>



Member State	Response
	<p>The Electronic Register of AFIR correspondence with EPPO, DNA, DLAF, IPJ, OLAF, DG Agri and the ECA records all correspondence between the AFIR (headquarters, regional centres and county offices) and these institutions, correspondence which has or may have possible fraud in the implementation of EAFRD projects as its subject.</p> <p>Also, the local structures of the AFIR are required to report to the Director-General and Control and Anti-Fraud Directorate all situations in which CRFIR/OJFIR staff are asked to appear at the headquarters of the control or criminal investigation bodies in order to be consulted on aspects relating to the projects implemented and/or the work carried out depending on the duties of the service, irrespective of the type of judicial procedure.</p> <p>- MIPE – AM POCU: Through regular working meetings</p>
PT	<p>The NAFS includes a specific measure on the general use of all tools made available by the European Commission for the purposes of assessing and mitigating the risk of fraud, particularly ARACHNE and OLAF's Early Detection and Exclusion System (EDES) database. The systems covered by Portugal 2030 are already sending data to ARACHNE.</p>
LV	<p>Ensuring access to various databases of national importance, introducing automatic controls is a determining factor for both fraud prevention, detection and investigation and it is included in the NAFS. In the NAFS period from 2024 to 2026, it is planned to continue optimizing the use of available national information systems for combating fraud, analysing which national information systems could still be interconnected and what are the problems of data analysis, as well as identifying opportunities for automatic controls.</p>
IT	<p>On this point, the situation in Italy is that there is a comprehensive system that fully meets the need to prevent and combat fraud against the EU. Each institution, agency and body responsible for managing EU resources in various capacities and according to various remits has set up over time – as part of an ongoing process of digitalising the fight against fraud – many systems, applications and databases, as well as methods and procedures, to properly ensure prior assessment of the risk of fraud, corruption, conflicts of interest and double funding in connection with EU budget implementation.</p> <p>With regard to budget revenue and specifically traditional own resources, the Customs and Monopolies Agency has reported that risk analysis activity in 2023 was based on examining the main information sources, with particular focus on information from reliable sources such as OLAF (around 50 INF MA mutual assistance reports) concerning all of the main financial risk areas: evasion of anti-dumping duties or countervailing duties, under-invoicing, misclassification of goods, abuse of preferential origin, abuse of procedure 42/63.</p> <p>Analysis of the INF MA reports triggered the following activities:</p> <ul style="list-style-type: none"> <li>- addition of more than 300 new risk profiles (relating to goods or to natural/legal persons);</li> <li>- amendment and/or recalibration of almost 400 existing risk profiles.</li> </ul> <p>In addition, more than 300 RIFs (Risk Information Forms) were issued via CRMS2 (Customs Risk Management System 2.0). These concerned tax-related risks and led to the addition of around 80 new risk profiles.</p> <p>What is more, risk profiles are still in place for the fight against under-invoicing using various control strategies targeting both goods and persons.</p> <p>As regards checks when customs declarations are submitted, the fight against under-invoicing follows two parallel tracks:</p>

Member State	Response
	<ul style="list-style-type: none"> <li>- for the first track, the analysis tool used to identify value thresholds is the dashboard in the THESEUS database provided by the Commission;</li> <li>- the second track uses CREDIBILITY, a new tax monitoring methodology for the fight against under-invoicing that was developed by the Agency. On the issue of e-commerce, a risk analysis strategy based on a statistical approach is being developed and tested with the aim of identifying any anomalies in the value of imports.</li> </ul> <p>The statistical analysis is based on processing a significant quantity of data on e-commerce extracted from the Cognos Datawarehouse on the basis of analysis of the H7 dataset. With informatics support from specific artificial intelligence algorithms based on the programming language Python, the statistical analysis aims to identify items/declarations with anomalous unit values (€/kg) ('outliers'), i.e. values below a given threshold or above a given ceiling.</p> <p>During 2023, work also continued on assessing risks using some specific methodologies in use at the Agency. These include the Fiscal Vigilance methodology. This consists in an analysis application which, using various search criteria such as the 10-digit customs code (TARIC) and the country of origin, calculates the 'threshold value' of goods via an algorithm based on the maximum number of transactions in a given period of time (usually two months). The 'threshold value' or statistical limit value is the value beneath which an amount entered on a declaration is considered to be an under-invoicing risk. The algorithm subdivides the transactions carried out into percentiles (calculated on a base of 10 or 100) and, by applying Gaussian distribution (a bell curve representing a precise statistical curve), calculates the values that are at either end of the curve and thus considered borderline cases and/or anomalous values. The application can also be used to adjust the risk profiles by 'categorising' the findings of checks. Every finding of a checking activity is 'categorised' as either compliant or non-compliant and according to the type of non-compliance (nature, quantity, value). At the end of the categorisation, the application is asked to calculate the threshold value with which the profile should be associated (for a given profile, declarations are selected based on the '&lt; threshold value' criterion, meaning that if the value declared is less than ('&lt;') the 'threshold value', it is deemed to be a case of under-invoicing).</p> <p>Another interoperability system and tool used for risk analysis is the aforementioned Customs Risk Management System (CRMS). This EU system for sharing risk reports between the Member States allows the customs authorities and the Commission to cooperate and priority control areas and crises to be managed. This application is hosted on a dedicated, protected network and allows the Member States to exchange risk information in real time.</p> <p>The CRMS comprises various domains designed for different purposes:</p> <ul style="list-style-type: none"> <li>- RIF (Risk Information Form): for exchanging information received from all Member States on tax and non-tax frauds;</li> <li>- CM (Crisis Management): crisis management dashboard (e.g. COVID, etc.);</li> <li>- PCA (Priority Control Area): priority control areas determined by the European Commission;</li> <li>- RMCS (Risk Management Collaboration Service): a collaboration request (CLR) is created when it is deemed necessary to request an action or some information to confirm the risk indicator or anomaly for a specific consignment, whether incoming, in transit or outgoing;</li> <li>- PRCI (Platform of Risk and Control Information): where specific risk detection methods exist (X-Ray Risk Form, K9 'Canine' Cases Form and Rummage Cases Form).</li> </ul> <p>Platform members add other details on risks using messages and secure email. Further assistance in mitigating the risk of fraud comes from 'reports' and 'searches' on the platform concerning all types of infringements.</p>

---

**Member  
State****Response**

---

In the same year, the Anti-Fraud Directorate trialled an Excel spreadsheet for the LEA (Logic, Experience and Analysis) project, which gives concrete form to a risk matrix aimed at the development of predictive models by:

- using an overall set of information that can be derived from the databases available to the Agency concerning imports, exports, cash import declarations and citations for cash import infringements;
- obtaining open-source information concerning economic studies, statistical publications, etc., so as to analyse potential inconsistencies (concerning individual persons or general categories of ATECO code or business/goods sector) in the relationship between cross-border movements of cash and the income declared by the offender or the person engaged in transit.

The risk matrix was used in 2023 in relation to various reports sent to the national financial intelligence unit (FIU) in order to prevent and combat money laundering linked to tax evasion and/or other serious tax and non-tax offences potentially involving cross-border movements of cash. The trialling of the LEA project led to dozens of reports also being sent to the Public Prosecutor's Office's Anti-Mafia and Anti-Terrorism Directorate and the local offices of the Customs and Monopolies Agency responsible for border crossings in order for targeted checks to be carried out on movements of cash and goods deemed to pose a risk of tax evasion, customs infringements linked to the taxable amount (under-invoicing or over-invoicing), infringements linked to the nature, quantity and origin of the goods declared for import and export, and money laundering.

Work is also being done to deploy the LEA model for the purposes of applying Article 7 of Regulation (EU) 2018/1672 and thus temporarily detaining cash that is moved cross-border in a suspicious manner.

Again with regard to budget revenue, and specifically VAT, the Revenue Agency has taken specific steps to prevent losses to the exchequer as a result of intra-EU VAT fraud by ensuring that national entities that commit VAT evasion by operating as shell companies in fraudulent schemes ('missing traders' or 'defaulters') have their VAT number swiftly cancelled or are excluded from VIES (VAT Information Exchange System) pursuant to Article 35(15-bis) of Presidential Decree No 633/1972 and the new paragraphs 15-bis-1 and 15-bis-2 (introduced with effect from 1 January 2023). In this context, particular emphasis was placed on data from electronic invoices issued and received and on some innovative tools for cooperation with other European countries. With regard to the database of electronic invoicing data, since 2023 it has been possible to access, under certain conditions, specific data concerning the goods to which invoices relate. This allows for more detailed control and monitoring of the transactions carried out by high-risk entities.

The TNA (Transaction Network Analysis) tool developed by the European Commission for Eurofisc purposes continues to make a particularly important contribution. It makes it possible to obtain information from the VIES of all EU Member States and analyse that information in one go. Intensive work continues to fight VAT fraud committed through the submission of false letters of intent. The entities posing the highest risk were identified thanks to timely analysis of all declarations of intent sent and, once irregularities were proven, formal notices were issued, and warning letters were sent to the sellers so as to stop the flow of fraudulent invoices and prevent further losses to the exchequer. The extent of the phenomenon has reduced significantly in the fuel sector thanks to the introduction of Article 6 of Decree-Law No 124/2019, and the sectors most affected are the clothing and clothing accessories sectors.

The intention for the coming years is to strengthen the activities described above by stepping up risk analysis activities, including new AI and machine learning tools. In terms of technology, a new anti-fraud analysis tool, TAXNET, is fully operational. Through the interoperability of various databases (electronic invoices, declaration data, personal data, bank transfers, VIES, etc.), it makes it possible

---

---

**Member  
State****Response**

---

to automatically reconstruct the entire fraud chain and rapidly map the links and recurrent connections between the various entities (natural and/or legal persons) involved in fraudulent transactions.

With regard to budget expenditure, risk assessment in relation to cohesion policy funding is one of the main control functions of the various managing authorities. The MAs widely apply EGESIF Guidance Note No 14-0021-00 issued by the European Commission on 16 June 2014 and concerning 'Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures' and extensively use Arachne.

The Arachne risk assessment system was developed by the European Commission to help Member States prevent fraud. It processes and analyses the data provided by EU countries on beneficiaries, contractors and other project stakeholders and carries out cross-checks between that data and information from external databases on undertakings and linked persons, making it possible to identify projects, beneficiaries and contractors posing a fraud risk.

Originally developed for the cohesion policy, the tool was extended to the CAP via a pilot project launched in February 2019 for rural development projects. Various national administrations expressed the need to have uniform national guidance on how to use Arachne as a tool to improve the identification, prevention and detection of fraud, in line with the requirements of their respective management and control systems. To answer this need, the administrations were notified of the establishment of a technical working group for this purpose chaired by the Inspectorate-General for Financial Relations with the European Union at the State General Accounting Department, which comes under the Ministry of Economic Affairs and Finance, and made up of representatives of several managing authorities and audit authorities for ERDF and ESF operational programmes 2014-2020, the Agency for Territorial Cohesion and the National Agency for Active Labour Market Policy.

That working group, which was established by Decision of the Head of the State General Accounting Department of 18 January 2019, drew up the 'National guidelines for using the EU anti-fraud system Arachne'. Aimed at managing authorities, certification authorities, audit authorities and the intermediate bodies of operational programmes, those guidelines provide specific guidance on how the use the tool so as to help ensure compliance with anti-fraud legislation.

In relation to their respective management and control systems, each administration, on the basis of its internal organisation, structural staffing level, and verification and oversight requirements, was able to choose the administrative stages at which the system would be used, in line with the existing specifications of EGESIF Guidance Note No 14-0021-00 of 16 June 2014.

At central level, as part of its role of coordinating authorities and audit functions, the Inspectorate- General for Financial Relations with the European Union (IGRUE) (part of the State General Accounting Department, which comes under the Ministry of Economic Affairs and Finance) issued its own Handbook of Audit Procedures 2021-2027 of 29 February 2024, which includes a specific section on risk assessment.

In this context, IGRUE has developed a national risk assessment methodology, available on the MyAudit information system, which has a greater level of detail, and some differences compared to the methodology set out in the aforementioned EGESIF Guidance Note, especially as regards the method for calculating the risk score.

IGRUE is also responsible for managing the Single Database (BDU), which contains all information on the planning and implementation of measures financed with regional policy funding from EU and national sources.

The Guardia di Finanza has economic/financial police functions that cover all types of infringement against the national and European budget, and as a result it carries out risk analysis and assessment

---

---

**Member  
State****Response**

---

activities in respect of both revenue and expenditure.

In order to combat VAT fraud, the Special Unit for Protecting Revenue and Combatting Tax Fraud conducts ongoing risk analysis to identify undertakings presumed to be involved in fraudulent schemes and then charges the force's local departments with carrying out the necessary investigations.

This analysis is based, firstly, on an examination of information from the Eurofisc network, as part of which the aforementioned TNA platform has been running since 2021. This makes it possible to use advanced analysis tools to rapidly and specifically identify potential cases of intra- EU VAT fraud.

This information is cross-checked against search results from the many databases to which the Guardia di Finanza has access, including:

- the STAF (Anti-Fraud Tool) application, which ensures effective monitoring of VAT- registered taxpayers so as to promptly identify entities involved in tax fraud and assign a risk score to each of them;
- - the Invoices and Payments portal and the @-Fattura [@-Invoice] application, which allow targeted and integrated analysis of electronic invoice data;
- - the EMCS-eAD Dogane [Customs] and COGNOS - Dogane e Accise [Customs and Excise] applications, which make it possible to monitor the circulation of products subject to excise duty and operators in the sector. These applications are particularly useful in the fight against VAT fraud relating to fuels;
- - COGNOS - area Analisi libera Italia [Italy free analysis area], a partition of the 'Customs declarations' section of the COGNOS business intelligence platform, which makes it possible to carry out multidimensional processing using historical customs declaration data concerning the month preceding the query. It is especially useful for selecting entities for post-clearance customs controls, for conducting any subsequent in-depth investigations and for carrying out any other investigative activities requiring the reconstruction of international trade flows, including from past periods.

Further specific analyses have been developed by the Special Unit for Protecting Revenue and Combatting Tax Fraud so as to combat undue offsetting and fraud in the assignment to third parties of building and energy tax credits, including the '110% Superbonus' scheme co-financed by the National Recovery and Resilience Plan (NRRP). Some of the main applications used for this are:

- P. Ris. M.A. - Collections, Monitoring and Applications Portal, which allows precise consultation of taxpayers' subsidised tax credits and data on assignments of credits to third parties;
- Moni. C. - Monitoring of Offsetting, which allows both individual and bulk searches to be carried out by processing the data from F24 tax payment forms to detect undue offsetting of tax credits.

Another key tool for risk analysis in the area of tax is the record of accounts with financial institutions, which is linked to the Revenue Agency's Tax Register. The record of accounts with financial institutions is organised on the basis of the tax code of each person holding an account. Every month, financial institutions send data concerning accounts and non-account transactions (transactions carried out directly at the bank counter using bank drafts or cash) and personal data on the persons linked to the account, specifying their role.

Every year, meanwhile, financial institutions send data on account balances, both the opening balance as of 1 January and the closing balance as of 31 December of the year to which the communication relates, or, for accounts closed during the year, the opening balance and the balance booked prior to the date of closure. Also sent are the total values of movements, broken down into debits and credits, the annual average deposits held in bank and post office deposit and current accounts, and other accounting data for other types of account.

---



For particular types of accounts with banks or other financial institutions, there is a requirement to send further data in addition to the data on deposits and annual flows. For example, for safe deposit boxes, the bank must report how many times the taxpayer accessed the box during the year.

The financial institutions required to send periodic reports to the record of accounts with financial institutions belong to various different categories, with the main ones being banks, the Italian post office, mutual guarantee societies and cooperatives, investment companies, collective investment undertakings (CIUs and SICAVs), asset management companies (AMCs), trusts, and insurance companies and institutions as regards their financial activities. The record of accounts with financial institutions is currently used for financial investigations, to draw up selective lists for tax evasion risk analysis and for the checks and controls carried out for the purposes of the ISEE (Equivalent Economic Situation Indicator). Recently, revenue collection agents have made increased use of the data in the record of accounts with financial institutions in procedures to enforce attachment orders against third parties, since it is debtors' bank accounts that are attached.

As regards digitalisation and the use of new tools aimed at improving interoperability between systems in the fight against customs fraud, the Customs Agency has launched a project to digitalise the customs procedures for loading/unloading and entry/exit from ports. During the development of this initiative, which is already in operation at the port of Bari and is being gradually extended to other ports (Ancona, Livorno and Venice), the MRN (Movement Reference Number) has been entered in each customs declaration processed by the competent offices. This is a unique identifier created by the customs systems when a declaration is submitted for the import, export or internal/external transit of goods. It makes it possible to identify, at any moment, the consignment with which the declaration is associated. The identifier is also available in a live environment in AIDA (Integrated Customs and Excise Automation).

This new development simplifies operations at customs posts, as the Guardia di Finanza officers responsible for affixing the 'exit stamp' can read the barcodes on customs declarations using e.g. optical readers and thus access information on the consignment more quickly.

In relation to public expenditure, a memorandum of understanding has been signed with the State General Accounting Department at the Ministry of Economic Affairs and Finance with the aim of regulating cooperation on making data available, establishing suitable access procedures and ensuring interoperability of information systems. In this context, a Technical Committee has been set up to determine the arrangements for implementing the agreement. The application envisaged by the agreement encompasses:

- the Guardia di Finanza dashboard in BDAP (Database of the Public Administration), which is a single standardised and streamlined tool for surveying, measuring and analysing the public finances. It makes it possible to carry out precise searches for data on payments made by the central administrations to the beneficiary concerned, in the financial years selected, with the data then being further processed using predefined 'analysis contexts';
- the aforementioned BDU-IGRUE, the Single Database of the General Inspectorate for Relations with the European Union at the State General Accounts Department, which collates data on the payments made under the operational programmes financed by the structural funds. This data is used by the Guardia di Finanza to populate the Anti-Fraud Information System (SIAF) discussed below;
- ReGiS, the platform that all parties involved (central administrations and implementing bodies) must use for management, reporting, control and monitoring activities linked to NRRP initiatives.

To make the prevention and combatting of fraud against EU budget expenditure more effective, the Special Unit for Public Expenditure and Combatting Fraud against the European Union handled the evolutionary maintenance of SIAF (Anti-Fraud Information System), which was created as part of a

---

project financed under the National Operational Programme ‘Governance’ and Technical Assistance 2007-2013.

SIAF is a business intelligence platform that supports operational analyses in the field of public expenditure. By collating the information obtained, including from the other databases used by the Guardia di Finanza, it is possible to extract lists of public funding beneficiaries potentially posing a risk of irregularities.

With specific reference to the NRRP, the Guardia di Finanza’s Special Unit for Public Expenditure and Combatting Fraud against the European Union, with the support of the Guardia di Finanza Unit at the Department for European Affairs at the Prime Minister’s Office, which acts as Technical Secretariat of COLAF, has prepared detailed checklists with specific risk indicators separately applicable to the disbursement of support or the performance of public works and the provision of services. Through the Network of NRRP Anti-Fraud Contact Persons established alongside the Coordination Committee for NRRP Reporting and Control by Decision No 57 of 9 March 2022, and through the ReGiS system developed by the State General Accounting Department, these checklists have been made available to all central and local administrations responsible for measures and to the implementing bodies involved in the implementation of the Plan, thus enabling those entities to improve their independent capacity to identify anomalous situations requiring further investigation.

An important new development in the measures taken by Italy to strengthen risk analysis in the management of EU funds is the Integrated Anti-Fraud Platform (PIAF-IT) developed by the General State Accounting Department in cooperation with COLAF and cofinanced by the European Commission (OLAF) with Hercule III funding. Specifically, PIAF-IT is an integration platform that extracts, aggregates and reconciles data from national sources (Revenue Agency, the Chamber of Commerce Information System (Infocamere), Court of Auditors) and EU sources (the Irregularity Management System (IMS), which directly comes under OLAF, and the Financial Transparency System (FTS), which is managed by the European Commission’s DG Budget in relation to beneficiaries of funds under direct management) to generate factsheets on natural or legal persons, providing a useful input for assessments of possible fraud. Its aim is to:

- intensify information exchange and thus strengthen the ‘fraud prevention’ stage as far as possible;
- centralise and make visible all key information on beneficiaries of EU public funding;
- develop specific outputs for analysing that information through a comparison against data in other databases via a search on a single information system, in an aggregated manner and without having to make several separate searches.

The platform is used as an effective tool supporting Arachne with the aim of consolidating and strengthening the fight against irregularities, fraud and other illegal activities against the EU budget both before expenditure is certified and during the ex-post control stage, as well as during administrative checks on implementation of the National Recovery and Resilience Plan. The technical context of PIAF-IT, which includes a microservices architecture able to store big data, has the following additional functionalities:

- it can be used to perform online searches (ordinary and historical views of natural or legal persons) and generate and display detailed factsheets;
  - it is highly extensible in the future to other data sources that would allow the entry concerned to be examined in greater detail as regards the person/activity involved (e.g. the data from the Ministry of Justice’s Criminal Records Information System concerning past convictions for specific offences involving fraud against the national and EU budget, and the Kohesio database managed by the Commission’s DG REGIO, which has up-to-date information on
-

Member State	Response
	projects and beneficiaries co-financed by the EU cohesion policy).
	<p>In addition, for 2024, in order to achieve ever-improved results in the fight against fraud, the Carabinieri confirmed the validity of its memorandum of understanding with AGEA (Agricultural Payments Agency). Under this memorandum, the fraud risk indicators for the CAP have been refined and the Criminal Focus Area dashboard has been further developed. Using aerial photographs, the dashboard records and analyses qualitative and quantitative changes in elements that point to criminal activity that hinders socio-economic development, identifying risk areas that require constant monitoring. The cooperation with AGEA is also making it possible to run a series of training events for all staff, enabling Carabinieri officers to deepen their knowledge of the new control tools being put in place by the Agency. In order to step up the fight against fraud, a licence to use the anti-fraud platform SAS was requested during a meeting with AGEA's Anti-Fraud and Risk Management Office.</p> <p>In 2024, the Cyber Investigation Section at the Operational Department of the Carabinieri Agri- Food Protection Unit became operational with the aim of training and upskilling officers to be deployed against threats coming from new IT technologies and enabling the use of investigation techniques and digital tools to be made available to the Carabinieri to fight crime committed using IT equipment.</p>

Q.2.3. If “NO” to Q.2.1, please explain why the digitalisation of the fight against fraud is not part of your NAFS nor of any other strategic approach.

Member State	Response
IE	Ireland does not have a NAFS; each MA has their own anti-fraud strategy for the protection of EU funds.
DE	<p>General comment: As a federal state, Germany does not have a national anti-fraud strategy. However, in this context, we would refer to Germany's Digital Strategy 2022-2025, p. 51 et seq. (<a href="https://digitalstrategie-deutschland.de/static/fcf23bbf9736d543d02b79ccad34b729/Digitalstrategie_Aktualisierung_25.04.2023.pdf">https://digitalstrategie-deutschland.de/static/fcf23bbf9736d543d02b79ccad34b729/Digitalstrategie_Aktualisierung_25.04.2023.pdf</a> + <a href="https://digitalstrategie-deutschland.de/">https://digitalstrategie-deutschland.de/</a>).</p> <p>Measures reported here have been taken at Länder level. Replies to Q 2.1 from the Länder (ERDF) range from 'Not yet, but we intend/are in the process of developing this part of the strategy' to 'NO'.</p>

Q.2.4 What are the main gaps you have identified in the digitalisation of your anti-fraud efforts?

Response	Frequency	Percentage	Member States
Difficulty in scaling digital solutions across the state	14	51.9%	HR, SE, BE, LT, CZ, ES, DE, BG, CY, EE, RO, PT, LV, IT
Lack of funding for digital tools	14	51.9%	HR, NL, EL, BE, FI, SI, CZ, ES,



Response	Frequency	Percentage	Member States
			SK, DE, BG, EE, RO, LV
Legal or regulatory barriers	14	51.9%	SE, NL, BE, LT, CZ, ES, SK, PL, DE, CY, EE, RO, LV, IT
Limited technical expertise within your organisation	14	51.9%	LU, HR, SE, NL, EL, FI, CZ, ES, HU, SK, DE, BG, MT, RO
Insufficient training for the staff and digital tools and processes	8	29.6%	HR, NL, CZ, ES, SK, BG, RO, LV
Outdated IT systems	8	29.6%	LU, NL, EL, SI, CZ, ES, CY, RO
No steps taken to identify gaps in digitalisation	6	22.2%	IE, FR, AT, SI, RO, DK
Resistance to change from the staffs and stakeholders involved	5	18.5%	LU, HR, SE, CZ, BG
Cybersecurity vulnerabilities	2	7.4%	CZ, RO

#### Q.2.5 What steps have you undertaken to address gaps in the digitalisation of your anti-fraud efforts?

Response	Frequency	Percentage	Member States
Training and development for staff	17	63.0%	SE, EL, BE, AT, FI, LT, SI, CZ, ES, HU, SK, DE, BG, MT, CY, RO, IT
Other (please specify)	9	33.3%	IE, SE, CZ, PL, MT, CY, EE, PT, DK
Conducted internal assessments or audits	8	29.6%	LU, EL, CZ, DE, EE, RO, DK, IT
Performed a gap analysis comparing the current capabilities with desired capabilities	8	29.6%	BE, SI, CZ, ES, SK, DE, RO, IT

Response	Frequency	Percentage	Member States
No specific actions taken yet to address gaps	5	18.5%	HR, NL, FR, ES, LV
Secured budget for digital improvements	5	18.5%	SI, CZ, MT, CY, RO
Developed a detailed digitalisation strategy addressing identified gaps	3	11.1%	CZ, ES, SK
Hired external consultants or experts	3	11.1%	LU, EL, CZ

Following Q.2.5, please specify "Other".

Member State	Response
IE	?
SE	There is ongoing cooperation with other authorities (the Swedish Agency for Economic and Regional Growth, the Migration Agency and the Swedish Board of Agriculture) owing to the lack of digital tools. Paving the way for future development, such as structured data based on data from applicants and introducing organisation registers that retrieve data from public databases. See also point 2.7.
CZ	Preparation of the complete digitalisation of administrative processes at prosecutorial level is ongoing. Links to external systems have been created (the Register of Beneficial Owners information system (ESM) and MS2021+, ARACHNE and MS2021+) and access has been ensured to the non-public part of the ESM and Register of Trust Funds information systems). Applications were procured for screening (CRIBIS) and using web interfaces for detecting fraud (such as double funding), use of the ESM. Information sharing has been expanded using cloud solutions.
PL	The Institution Coordinating the Partnership Agreement cooperates on an ongoing basis with national bodies external to the institutions of the management and control system in the transmission of information on entities and persons with links to those entities obtained from external registers managed by these institutions. Where required, the Institution Coordinating the Partnership Agreement concludes agreements on rules of cooperation with register-managing entities for the exchange of data necessary to carry out verifications in relation to the detection of conflicts of interest and the fight against irregularities and fraud.
MT	With reference to Question 2.4, notwithstanding that the Maltese AFCOS has limited technical IT expertise, it is being assisted by IMU within the Office of the Prime Minister. Furthermore, the co-ordination between the members of the Co-ordinating Committee facilitates knowledge sharing with respect to Information and Communication Technology (ICT).
CY	Steps are sectoral and there are no steps for mainstream programs.

Member State	Response
EE	We have begun reviewing our monitoring system to map out our current needs and subsequently implement changes, including addressing the need to enhance the fight against fraud through increased digitalization. Additionally, we are exploring greater opportunities for cooperation with investigative bodies, which already have the necessary tools and expertise. Including we are using internal risk analysis capabilities and Arachne.
PT	Contacts with public administration bodies have been established to improve and extend the set of interoperability solutions available/to be made available.
DK	The Danish Business Authority: We have made a fraud-risk assessment.

Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud? Inventory of existing tools: conduct a thorough inventory of existing digital tools and technologies used in the fight against fraud.

Response	Frequency	Percentage	Member States
Action taken	10	37.0%	SE, LT, SI, CZ, PL, DE, BG, MT, RO, IT
Action planned	9	33.3%	LU, HR, FR, AT, ES, HU, SK, CY, LV
Action not taken nor foreseen	8	29.6%	IE, NL, EL, BE, FI, EE, PT, DK

Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud? Benchmarking on new trends: conduct benchmarking research on new trends and technologies used in the fight against fraud.

Response	Frequency	Percentage	Member States
Action not taken nor foreseen	13	48.1%	IE, LU, HR, NL, EL, AT, FI, ES, PL, EE, PT, LV, DK
Action planned	9	33.3%	FR, BE, CZ, HU, SK, BG, MT, CY, RO
Action taken	5	18.5%	SE, LT, SI, DE, IT

Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Evaluation and updates of existing IT tools.

Response	Frequency	Percentage	Member States
Action planned	11	40.7%	LU, HR, FR, FI, LT, ES, BG, MT, CY, RO, PT
Action taken	10	37.0%	SE, BE, SI, CZ, HU, SK, PL, DE, LV, IT
Action not taken nor foreseen	6	22.2%	IE, NL, EL, AT, EE, DK

Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Development/deployment of new, dedicated IT tools.

Response	Frequency	Percentage	Member States
Action planned	11	40.7%	LU, NL, FR, BE, FI, LT, ES, DE, MT, RO, DK
Action not taken nor foreseen	9	33.3%	IE, HR, EL, AT, HU, BG, CY, EE, LV
Action taken	7	25.9%	SE, SI, CZ, SK, PL, PT, IT

Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Improve interoperability between systems already in use to enhance data sharing.

Response	Frequency	Percentage	Member States
Action planned	16	59.3%	LU, NL, FR, AT, FI, LT, CZ, ES, SK, DE, BG, CY, EE, RO, LV, DK
Action taken	8	29.6%	SE, BE, SI, HU, PL, MT, PT, IT
Action not taken nor foreseen	3	11.1%	IE, HR, EL

Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Dedicated allocated staff / resources / taskforce.

Response	Frequency	Percentage	Member States
Action taken	14	51.9%	SE, NL, BE, LT, SI, CZ, HU, SK, PL, DE, CY, PT, LV, IT
Action planned	8	29.6%	LU, HR, FR, ES, BG, MT, EE, RO
Action not taken nor foreseen	5	18.5%	IE, EL, AT, FI, DK

Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Trainings of the staff.

Response	Frequency	Percentage	Member States
Action taken	18	66.7%	SE, NL, BE, AT, LT, SI, CZ, ES, HU, SK, PL, DE, MT, CY, EE, LV, DK, IT
Action planned	7	25.9%	LU, HR, FR, FI, BG, RO, PT
Action not taken nor foreseen	2	7.4%	IE, EL

Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Risk analysis assessment.

Response	Frequency	Percentage	Member States
Action taken	17	63.0%	LU, SE, NL, BE, SI, CZ, HU, SK, PL, DE, MT, CY, EE, RO, LV, DK, IT
Action planned	7	25.9%	HR, FR, FI, LT, ES, BG, PT
Action not taken nor foreseen	3	11.1%	IE, EL, AT

Q.2.6. What actions have you taken or are you taking to keep up with evolving new technologies used to commit fraud?: Other (please specify in the next question).

Response	Frequency	Percentage	Member States
Action not taken nor foreseen	18	66.7%	IE, LU, HR, NL, FR, BE, AT, LT, ES, SK, PL, BG, MT, CY, PT, LV, DK, IT
Action taken	7	25.9%	SE, FI, SI, CZ, HU, DE, RO
Action planned	2	7.4%	EL, EE

Q.2.7 Following Q.2.6, please specify any other actions you have taken, or you have planned on taking to keep up with evolving new technologies used to commit fraud.

Member State	Response
IE	There is no national anti-fraud strategy in place,
LU	In addition to the actions described above, one stakeholder is in process of engaging an external consultant in anti-fraud matters and plans to recruit an anti-fraud officer in 2025.
HR	No other action is taken nor foreseen.
SE	<p>Paving the way for future development;</p> <ol style="list-style-type: none"> <li>1. Introducing an integrated organisation register in the My Application/Nyps aid case system that retrieves public data on the organisation. The payment method (bankgiro and plusgiro) of the applicant organisation is verified automatically through checks against external services.</li> <li>2. Reporting of data from the project in a structured way in My Application/Nyps.</li> <li>3. The structured data in Nyps has made it possible for us to check whether there is double reporting of certain costs in ERUF9. With the ProDiver analysis programme, which retrieves data from Nyps, we can systematically analyse data on personnel costs and actual costs and detect possible double funding.</li> </ol>
NL	N/a
EL	<p>Together with the AFCOS of Cyprus and the AFCOS of Bulgaria, the EYTHYPS is participating in the transnational project ‘Strengthening national anti-fraud strategies in the financial interests of the EU’, financed through the Technical Support Instrument (TSI) of the European Commission. The Directorate-General for Structural Reform Support (DG REFORM) of the European Commission is responsible and the OECD is the beneficiary. The project’s aim is ‘the improvement of national anti-fraud strategies and the development of a comprehensive methodology with clear procedures and indicators to support the monitoring, assessment and updating of national anti-fraud strategies, including capacity-building in relation to the use of the methodology’ and, specifically</p>

Member State	Response
	for Greece, the assessment of the National Anti-Fraud Strategy implemented in the ESPA, its updating and the development of a monitoring and assessment methodology.
BE	/
FI	Participation of national experts in the Commission's expert groups dealing with digital tools to protect the EU budget.
SI	In this moment we plan no further actions as mentioned in Q.2.6.
CZ	Training of an expert team of data analysts, implementation of new AI tools, architecture of electronic risk analysis strategy, development of own risk-analysis tools. A self-assessment system has been put in place in accordance with the Commission's guidelines. Staff participate not only in training specialised in fraud and fraud prevention, but also, for example, in the use of artificial intelligence, including training abroad. Furthermore, the managing authority prepares annual reports and evaluates the checks carried out under the Fraud Prevention Directive.
HU	Providing training on the application of artificial intelligence in the institutional system for development policy, not yet linked to specific workflows.
DE	The Federal Ministry of Food and Agriculture (BMEL) under 'Other': Use of new databases (e.g. the Transparency Register).
BG	N/A
MT	Not applicable.
EE	Developing risk systems in Customs and Tax areas - we are taking risk models to next SAS platform,
RO	<p>- AFIR: The Paying Agency for Rural Investments has international certification for the standard ISO 37001:2016, which is applicable to the anti-bribery management system.</p> <p>- MIPE - DGMMRR: Training planned at the start of 2025 with the Arachne team, analysis and verification of the information in the EDES Database - <a href="https://commission.europa.eu/strategy-and-policy/eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures/edes/edes-database_en">https://commission.europa.eu/strategy-and-policy/eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures/edes/edes-database_en</a></p>
IT	<p>As far as legislation is concerned, mention should be made of:</p> <p>1) Law No 90/2024 laying down provisions on strengthening national cybersecurity and on cybercrime. The changes made by this law are linked to the second recommendation in the 2023 PIF report, namely, to accelerate the digitalisation of the fight against fraud, specifically by strengthening national bodies' 'cyber resilience' measures and the tools for fighting cybercrime. Its provisions include, in particular:</p> <p>a) making penalties more severe and introducing aggravating circumstances for cyber offences (Articles 615-ter, 615-quater, 617-bis, 617-quater, 617-quinquies, 617-sexies of the Criminal Code);</p> <p>b) introducing, for cyber offences, the mitigating circumstance of particularly minor nature and cooperation; c) redefining the offence of damaging IT or electronic systems of public interest;</p> <p>d) coordinating with the new provisions on extending the end dates of investigations and on</p>

Member State	Response
	<p>maximum duration;</p> <p>e) extending to cybercrime the coordination role of the National Anti-Mafia and Anti- Terrorism Prosecutor, the provisions on state witnesses and criminals who turn state's evidence and the provisions on wiretapping for organised crime offences;</p> <p>f) extending corporate liability for cyber extortion offences;</p> <p>1) Decree of the Minister for Justice of 15 March 2024 establishing the national register of reports, documents and recordings of wiretaps carried out in proceedings in which the European Public Prosecutor's Office has exercised its power and any other documents related thereto. This provides for the units of the European Public Prosecutor's Office to use the recently established inter-district digital infrastructure to save all conversations and communications recorded with Public Prosecution Office equipment used to investigate the offences referred to in the PIF Directive.</p> <p>Also, on the issue of accelerating the process of digitalising the fight against fraud, the Department for Technological Innovation (DIT) at the Ministry of Justice has stated that:</p> <ul style="list-style-type: none"> <li>- the digitalisation of the fight against fraud has been ensured by structured monitoring of data on PIF offences using the applications made available to Italian law enforcement authorities (NDR), lawyers (PDP) and prosecutors/judges (REGWEB and APP);</li> <li>- the difficulties in rolling out digital solutions nationwide have been remedied by staff training and development;</li> <li>- so as to keep pace with the development of new technologies used to commit fraud, the action taken has been to draw up an in-depth inventory of the existing digital tools and technologies used in the fight against fraud, and to assess and update the existing IT tools and develop new bespoke IT tools;</li> <li>- the planned actions consist in making the systems already in use more interoperable so as to improve data sharing and staff training.</li> </ul> <p>Specifically, the creation of the criminal law data lake via the central applications of the Italian electronic criminal-law process (NDR, PDP and ADP) will make it possible to improve and broaden the quality of the data and, as a result, the activities of prevention, investigation and punishment.</p> <p>In addition, particular importance has been placed on the inventory of existing digital tools and technologies used in the fight against fraud, the setting up of a special task force, staff training and the assessment of risk analyses.</p> <p>Utmost importance has also been placed on comparative analysis of new trends, with comparative research into the new technologies used in the fight against fraud, and on how to make the systems already in use more interoperable so as to improve data sharing.</p> <p>Also in use are (integrated) automated data analysis tools, database integration and cybersecurity measures.</p> <p>Also planned are a system for managing fraud cases, data sharing between agencies and automation of information exchange.</p>

**Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Inventory of existing tools: conduct a thorough inventory of existing digital tools and technologies used in the fight against fraud**

Response	Frequency	Percentage	Member States
Important	14	51.9%	LU, HR, SE, NL, BE, LT, SI, CZ,



Response	Frequency	Percentage	Member States
			HU, SK, DE, BG, CY, EE
Very important	7	25.9%	FR, ES, PL, MT, RO, LV, IT
No opinion	3	11.1%	IE, EL, AT
Neutral	2	7.4%	PT, DK
Not important	1	3.7%	FI

Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Benchmarking on new trends: conduct benchmarking research on new trends and technologies used in the fight against fraud

Response	Frequency	Percentage	Member States
Important	13	48.1%	LU, SE, NL, BE, CZ, ES, HU, SK, DE, BG, CY, EE, LV
Very important	6	22.2%	FR, LT, SI, MT, RO, IT
Neutral	3	11.1%	HR, PL, PT
No opinion	2	7.4%	IE, AT
Somewhat important	2	7.4%	EL, DK
Not important	1	3.7%	FI

Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Evaluation and updates of existing IT tools

Response	Frequency	Percentage	Member States
Very important	14	51.9%	FR, BE, LT, SI, ES, SK, PL, DE, BG, MT, RO, PT, LV, IT
Important	7	25.9%	LU, NL, EL, FI, HU, CY, EE
Neutral	4	14.8%	HR, SE, CZ, DK

Response	Frequency	Percentage	Member States
No opinion	2	7.4%	IE, AT

Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Development/deployment of new, dedicated IT tools

Response	Frequency	Percentage	Member States
Important	11	40.7%	LU, HR, NL, EL, FI, LT, CZ, DE, BG, EE, PT
Very important	8	29.6%	FR, SI, ES, SK, PL, MT, RO, IT
Neutral	5	18.5%	SE, BE, CY, LV, DK
No opinion	3	11.1%	IE, AT, HU

Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Improve interoperability between systems already in use to enhance data sharing

Response	Frequency	Percentage	Member States
Very important	15	55.6%	LU, HR, SE, FR, EL, BE, SI, ES, PL, DE, MT, RO, PT, LV, IT
Important	10	37.0%	NL, FI, LT, CZ, HU, SK, BG, CY, EE, DK
No opinion	2	7.4%	IE, AT

Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Dedicated allocated staff / resources / taskforce

Response	Frequency	Percentage	Member States
Important	13	48.1%	SE, NL, EL, FI, SI, HU, SK, PL, DE, MT, EE, PT, LV

Response	Frequency	Percentage	Member States
Very important	9	33.3%	LU, HR, FR, BE, LT, ES, CY, RO, IT
Neutral	3	11.1%	CZ, BG, DK
No opinion	2	7.4%	IE, AT

Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Trainings of the staff

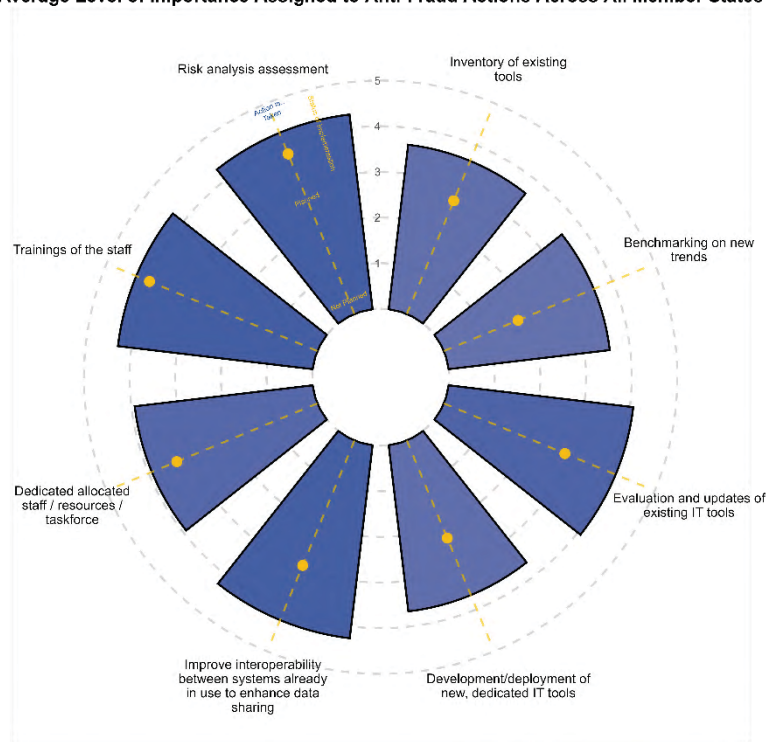
Response	Frequency	Percentage	Member States
Very important	16	59.3%	HR, NL, FR, BE, FI, LT, SI, ES, SK, DE, MT, CY, EE, RO, PT, IT
Important	9	33.3%	LU, SE, EL, CZ, HU, PL, BG, LV, DK
No opinion	2	7.4%	IE, AT

Q.2.8 Please indicate the level of importance you assign to each of the following actions in anti-fraud efforts.: Risk analysis assessment

Response	Frequency	Percentage	Member States
Very important	17	63.0%	LU, HR, NL, FR, EL, BE, SI, ES, SK, PL, DE, MT, CY, EE, RO, PT, IT
Important	7	25.9%	SE, FI, LT, CZ, HU, BG, LV
No opinion	2	7.4%	IE, AT
Neutral	1	3.7%	DK

## Polar plot of the Average Level of Importance Assigned to Anti-Fraud Action

Average Level of Importance Assigned to Anti-Fraud Actions Across All Member States



The responses start from 0 No Opinion and then range from 1 Not Important to 5 Very Important.  
The point on the line indicates the average level of implementation of the corresponding action with the levels:  
Action not taken nor foreseen, Action planned and Action Taken

### Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Use of AI (Artificial Intelligence)

Response	Frequency	Percentage	Member States
Planned to use	13	48.1%	HR, SE, EL, LT, CZ, ES, SK, DE, BG, MT, EE, RO, PT
Not used / Not planned to use	9	33.3%	IE, LU, NL, BE, AT, FI, HU, CY, DK
Used	5	18.5%	FR, SI, PL, LV, IT

Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Data Analysis tools (external)

Response	Frequency	Percentage	Member States
Used	23	85.2%	LU, HR, SE, NL, FR, EL, BE, AT, LT, SI, CZ, ES, HU, SK, PL, DE, MT, CY, EE, RO, LV, DK, IT
Not used / Not planned to use	3	11.1%	IE, FI, BG
Planned to use	1	3.7%	PT

Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Automated data analysis tools (integrated)

Response	Frequency	Percentage	Member States
Used	13	48.1%	SE, NL, FR, BE, LT, SI, CZ, HU, SK, PL, DE, RO, IT
Planned to use	11	40.7%	LU, HR, EL, FI, ES, BG, MT, EE, PT, LV, DK
Not used / Not planned to use	3	11.1%	IE, AT, CY

Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Predictive analytics

Response	Frequency	Percentage	Member States
Not used / Not planned to use	12	44.4%	IE, LU, NL, BE, AT, FI, HU, PL, BG, MT, CY, DK
Planned to use	9	33.3%	HR, EL, CZ, ES, DE, EE, PT, LV, IT
Used	6	22.2%	SE, FR, LT, SI, SK, RO

Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Database integration

Response	Frequency	Percentage	Member States
Used	16	59.3%	SE, FR, BE, LT, SI, CZ, ES, HU, SK, PL, BG, MT, EE, RO, PT, IT
Planned to use	7	25.9%	LU, HR, NL, EL, DE, CY, LV
Not used / Not planned to use	4	14.8%	IE, AT, FI, DK

Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Fraud case management system

Response	Frequency	Percentage	Member States
Used	16	59.3%	LU, NL, FR, EL, BE, LT, CZ, ES, HU, DE, BG, MT, EE, RO, LV, IT
Not used / Not planned to use	6	22.2%	IE, AT, FI, SK, CY, DK
Planned to use	5	18.5%	HR, SE, SI, PL, PT

Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Cross-agency data sharing

Response	Frequency	Percentage	Member States
Used	16	59.3%	LU, NL, EL, LT, CZ, HU, SK, PL, DE, BG, MT, EE, RO, PT, DK, IT
Planned to use	8	29.6%	HR, SE, FR, BE, SI, ES, CY, LV
Not used / Not planned to use	3	11.1%	IE, AT, FI

Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Cybersecurity measures

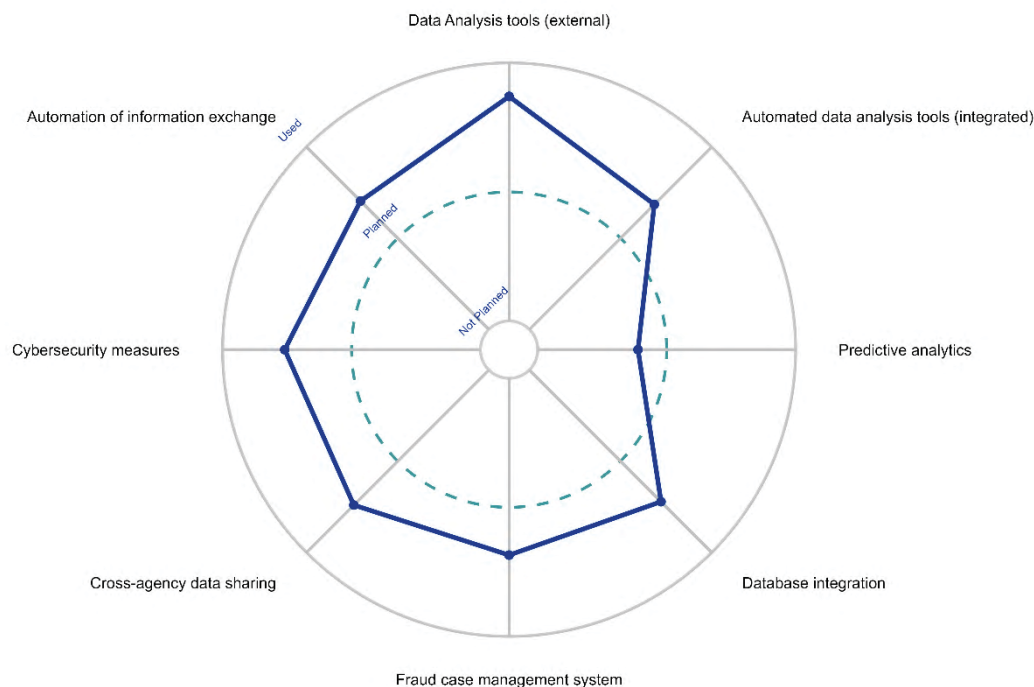
Response	Frequency	Percentage	Member States
Used	19	70.4%	LU, SE, NL, BE, LT, SI, CZ, ES, HU, SK, PL, DE, BG, MT, EE, RO, PT, LV, IT
Not used / Not planned to use	5	18.5%	IE, AT, FI, CY, DK
Planned to use	3	11.1%	HR, FR, EL

Q.2.9 Which digital tools or technologies are currently in use or planned for use in your anti-fraud efforts?: Automation of information exchange

Response	Frequency	Percentage	Member States
Used	15	55.6%	SE, NL, FR, BE, LT, CZ, ES, HU, SK, PL, MT, EE, RO, PT, IT
Planned to use	8	29.6%	LU, HR, EL, SI, DE, BG, CY, LV
Not used / Not planned to use	4	14.8%	IE, AT, FI, DK

## Spiderplot of Average Stage of Implementation of Digital Tools and Technologies Across All Member States

Average Stage of Digital Tools and Technologies Across All Member States



The Graphic illustrates the status of implementation of tools and technologies in levels include 'Not Planned', 'Planned' and 'Used'

Q.2.10 Following Q.2.9, please specify any other digital tools or technologies you are using, or you are planning to use.

Member State	Response
IE	There is no national anti-fraud strategy in place, it is hard to answer these questions where there are a number of MAs with responsibility for managing EU funds
HR	Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development is using POWER BI (OLAP) tool.
SE	A simpler analysis model in ProDiver.
NL	Planning to use new ARACHNE
FR	Within the framework of the NAFS, use of the Transaction Network Analysis (TNA) tool or of data from EUCARIS (the system for sharing data on driver's licences and registration documents among EU Member States) to combat VAT fraud.
EL	The EYTHYPS and the ESPA authorities use automated information exchange in the field of expenditure.
BE	Calista, Arachne



Member State	Response
AT	Arachne
FI	The possibility of introducing the ARACHNE system will be explored.
SI	Financial Administration of the Republic of Slovenia: Digital tools - platforms, which are used in FARS are SAP Business Intelligence – BOBJ, QlikView, QlikSense and KNIME, which can all be bought on the market. These tools access different internal and external data sources. These sources are further digital treated within specific IT program codes (scripts), which are written upon the specific needs within the self-developed applications. Applications are usually daily overnight updated.
CZ	<p>Use of links to external systems (the Register of Beneficial Owners information system (ESM) and MS2021+, ARACHNE and MS2021+) as well as use of access to the non-public part of the ESM and Register of Trust Funds information systems. Use of the CRIBIS application, use of Arachne, use of web interfaces to detect, for example, double funding: <a href="https://dotaceeu.cz/cs/statistiky-a-analyzy/mapa-projektu">https://dotaceeu.cz/cs/statistiky-a-analyzy/mapa-projektu</a>, <a href="https://red.financnisprava.cz/">https://red.financnisprava.cz/</a>, <a href="https://kohesio.ec.europa.eu/en/projects">https://kohesio.ec.europa.eu/en/projects</a>.</p> <p>The public prosecution service is preparing the digitalisation of internal administrative processes; this involves an in-house tool not directly linked to the systems of other public authorities, which is also motivated by the nature of criminal proceedings and the nature of the performance of the activities of the public prosecution service.</p>
HU	The Development Policy Database and Information System (FAIR), the European Union Programme System (EUPR), which includes a fraud prevention function, and also ARACHNE.
SK	Various Slovak authorities, including the audit authority use the Arachne tool and following websites to verify information: <a href="http://www.transparex.sk">www.transparex.sk</a> , <a href="http://www.orsr.sk">www.orsr.sk</a> (Business register), <a href="http://www.zrsr.sk">www.zrsr.sk</a> (The trade register), <a href="http://www.foaf.sk">www.foaf.sk</a> and <a href="http://www.oversi.gov.sk">www.oversi.gov.sk</a> .
PL	None
DE	<p>The Federal Ministry of Food and Agriculture (BMEL): Use of national databases and registers (e.g. the Transparency Register, the Trade Register).</p> <p>The Lower Saxony ERDF Managing Authority: The processes and procedures for handling and managing the multi-fund programme 2021-2027 in Lower Saxony are supported by different IT systems. The Investitions- und Förderbank Niedersachsen (NBank) uses the ABAKUS accounting system. On basis of the ABAKUS, the additional IT system NIBAS (Lower Saxony Information, Reporting and Billing System) was developed, which includes in particular the areas of evaluation and supplementary areas of application. In addition to the accounting and settlement systems (ABAKUS and NIBAS), there is also increased digitalisation in NBank's funding processing as part of IT security, which also has an impact on anti-fraud. Among other things, a digital application is made possible by NBank's IDA customer portal, which is intended to simplify the application and project processing. In addition, suspected fraud is reported online via digital means to the competent authorities and institutions.</p> <p>The Schleswig-Holstein ERDF Managing Authority:</p> <ul style="list-style-type: none"> <li>- Authentication via the service portal;</li> <li>- safeguards, such as the use of TLS certificates for encrypted communication.</li> </ul>

Member State	Response
MT	<p>(i) Scarlet: a data mining app aggregating shareholding information available on the Malta Business Registry in order to understand any linkages between Malta-based enterprises registered on the MBR and their shareholders, and the composition of the respective undertaking and its UBOs thereof;</p> <p>(ii) Malta Association for Credit Management (MACM): a website which provides information on Malta-based enterprises' VAT number and whether enterprises or individuals have had any court orders or notices, dishonoured cheques, creditors, judicial letters or civil cases;</p> <p>(iii) The Public Employment Service database: this database provides the employment history on any individual which is under scrutiny.</p>
EE	Tax and Customs colleagues are testing machine learning and network analysis tool.
RO	<p>-AFIR: I. The AFIR IT system:</p> <p>1) The rural development claim processing system (SPCDR) with the following main modules:</p> <p>a) Submission and evaluation of the funding application, including the project selection and resolution of challenges to the assessment of the funding application,</p> <p>b) Signing and amendment of the funding contract, c) Procurement, d) Payment authorisation, e) Ascertainment of irregularities, f) Establishing debt and debt recovery.</p> <p>FUNCTIONALITY: recording of funding applications in the AFIR IT system and their assessment, verification of eligibility and of selection criteria for the projects submitted, submission of the proposal for the on-site visit and drafting of reports following on-site visits, drafting of assessment reports, selection and responses to assessment, notifying applicants of the status of their funding application, settlement of appeals, drafting and signing of contracts/financing decisions/additional documents, submission and verification of procurement documents, submission of payment instalment declarations and of payment application documents, preparation of orders, payment certificates and orders for payment to beneficiaries, recording in the accounts of the payments made, the constitution of debts and their recovery, reports to the European Commission. In the SPCDR, applicants/beneficiaries of grants can submit documents relating to all stages of project implementation online.</p> <p>2) The online reference price database ensures access to information for applicants for European funding, at the same time simplifying the procurement procedure. It will be possible for the elements found in this database to be purchased by private NRDP beneficiaries, directly, without going through any other procurement procedure. The database is structured in line with the following criteria: CPV code, make, model, standard equipment and price in euro (or USD), excluding VAT. The identity of the person submitting the data remains confidential. The AFIR ensures that the online reference price database is completed through the collection, verification and validation of offers sent by the manufacturers, importers or distributors of vehicles, tools, specialised equipment, greenhouses, silos, buildings, sheds and furnishings. The AFIR conducts additional checks of the prices submitted and enters prices in the database which may have been found to be lower than those initially presented by the tenderer. Where the AFIR finds differences between the prices communicated and those practised on the market, the checks will be extended to all the prices communicated and, until the checks are finalised, will exclude from the database all equipment communicated by the manufacturer, importer or distributor in question. In order to offer interested parties, the possibility of comparing equipment from the database, the degree of accuracy of the information entered needs to be improved, and the information on the characteristics and</p>

Member State	Response
	<p>performance of the equipment included in the online reference price database also needs to be standardised. To this end, technical sheets have been developed setting out the minimum obligatory information to be provided concerning the degree of equipment of the elements entered or to be entered in the database with AFIR reference prices.</p> <p>3) The application for the on-site visit for mobile devices ensures that AFIR experts take photographs of the project implementation locations and send them to the SPCDR.</p> <p>4) The registry ensures that the input/output/document transfer flows at AFIR level are recorded.</p> <p>5) The accounting of payments from European funds ensures a record of the funding of the accounts from which payments are made to beneficiaries, and the preparation of payment orders.</p> <p>6) The financial accounting system of the AFIR ensures the processing and recording of financial accounting activities in the county offices, regional centres and central headquarters of the AFIR.</p> <p>II. ARACHNE. III. COLLABORATION PROTOCOLS: The purpose of these protocols is the exchange of databases/access to databases for both the 2014-2020 NRDP and the SP CAP 2023-2027. They have been concluded with the following institutions: the ONRC, the National Labour Inspectorate, the National Veterinary Health and Food Safety Authority, the Ministry of Health and the National Environment Agency and the National Environmental Guard, the MDLPA and the National Investments Company, APIA, the Competition Council, the DG for Persons' Records, ANAF and the EPPO.</p> <p>- DGP-AM POPAM: The website <a href="http://www.romanian-universe.ro">www.romanian-universe.ro</a> used for the collection of data and information. We intend to regain access to RECOM by signing a protocol with the ONRC, and also REVISAL and ARACHNE.</p> <p>- MDLPA: Joint Electronic Monitoring System for the period 2021-2027, Electronic Monitoring System for the period 2014-2020</p> <p>- MIPE – AM POCU: SMIS, ARACHNE, SFC, SICAP, RECOM</p> <p>- MIPE - DGMMRR: Arachne (under development), AFIS-IMS</p>
LV	Arachne and nationally available information systems (e.g. e-cohesion, Electronic Procurement System, System of the Tax Authority, Enterprise Register, etc.).
DK	The Danish Agency for Green Land Conversion and Water Environment: We are examining the potential use of ARACHNE for identifying red flags regarding fraud and circumvention.
IT	<p>The managing authority of the Ministry of Education and Merit's NOP/NP 'School' has adopted a digital transformation strategy that aims to make control procedures more effective by digitalising them through solutions that use AI to check the documentation submitted by beneficiaries, systems for automating data entry through optical character recognition (OCR), checks that can be automated through interoperability and, in general, the (at least partial) automation of controls.</p> <p>In addition, the Ministry of Justice has stated that the Senate is currently examining a draft law laying down provisions, and delegating power to the government, in relation to AI. In light of the recommendation to accelerate the digitalisation of the fight against fraud, the provisions of this draft law include delegating power to the government to systematically define rules for cases where AI systems are used for unlawful purposes. The delegation 'constitutes a supplementary measure that provides for the introduction of an offence, a generic aggravating circumstance and specific aggravating circumstances for certain offences.</p>

Member State	Response
	<p>More specifically, the delegated legislator has been called upon, firstly, to provide for tools in civil, administrative and criminal law, including interim measures, aimed at removing, and preventing the spread, of content generated illegally, including with AI systems, backed up by a system of effective, proportionate and dissuasive penalties.</p> <p>In addition, the government will have to introduce one or more separate offences, penalised as either deliberate or negligent acts, consisting in the failure to adopt, or failure to update, security measures for the production, release and professional use of AI systems and further offences, penalised as deliberate acts, intended to protect specific legal interests that are at risk of being compromised through the use of AI systems and cannot be properly protected by prosecuting existing offences.</p> <p>Thirdly, when the delegation is exercised, a specific aggravating circumstance will have to be introduced for deliberate offences subject to penalties other than life imprisonment, in which the use of AI systems contributes very seriously to the damage done to the protected legal interest, including cases of damage to interests of persons or the State.</p> <p>Lastly, in order to bring about an overall rationalisation of the system, the delegated legislator has been called upon to review the substantive and procedural legislation in force concerning the introduction of a generic aggravating circumstance where an offence is committed using AI systems; the introduction of a new offence of unlawful distribution of content generated or manipulated with AI systems; the insertion into the Criminal Code of specific aggravating circumstances linked to the use of AI systems in the commission of offences</p>

#### Q.2.11 Are your data analysis tools integrated directly into your databases, or do you deploy external systems for data analysis?

Response	Frequency	Percentage	Member States
External data analysis tools	15	55.6%	LU, HR, NL, BE, AT, LT, SI, CZ, DE, CY, EE, RO, PT, LV, DK
Other (please specify)	5	18.5%	SE, EL, ES, HU, MT
Not applicable	4	14.8%	IE, FR, FI, BG
Data analysis tools integrated to databases	3	11.1%	SK, PL, IT

Following Q.2.11, please specify "Other".

Member State	Response
SE	ProDiver is an external analytical tool that retrieves data from Nyps (support system)

Member State	Response
EL	Use of the fraud risk assessment tool (E.VIII.1_1), developed in Excel format. It captures and assesses the potential risks of fraud for the Programme and is based on a specific methodology developed by the European Commission (GUIDANCE NOTE ON FRAUD RISK ASSESSMENT AND EFFECTIVE AND PROPORTIONATE ANTI-FRAUD MEASURES (EGESIF 14-0021-00, 16/06/2014). It was used during the 2014-2020 programming period, updated in line with the new requirements, and is also being used in the 2021-2027 programming period.
ES	Most of the entities consulted have 'Data analysis tools integrated to databases'. In one case the answer was 'External data analysis tools'
HU	We also use data analytics tools integrated into databases and external data analytics tools.
MT	Our data analysis combines integrated and external tools. Malta uses the ARACHNE tool, which accesses data from the Maltese centralized information system, while additional analysis is conducted using external tools. Scarlet aggregates shareholding data from the Malta Business Registry to identify links between enterprises and their Ultimate Beneficial Owners. The Malta Association for Credit Management (MACM) provides insights into enterprises, including VAT numbers and any associated court orders or financial issues. The Jobsplus database offers employment history on individuals under scrutiny. This combined approach ensures comprehensive data-driven decision-making.

#### Q.2.12 Does your data management system facilitate interoperability?

Response	Frequency	Percentage	Member States
YES	16	59.3%	IE, LU, NL, FR, BE, AT, SI, CZ, HU, SK, PL, MT, EE, RO, PT, IT
NO	11	40.7%	HR, SE, EL, FI, LT, ES, DE, BG, CY, LV, DK

#### Q.2.13 If YES to Q.2.12, could you describe how interoperability is achieved between your data analysis tools and databases?

Member State	Response
IE	For example, the ESF+ permits interoperability as it is designed to comply RestAPI requirements on the Microsoft platform
LU	Analysis and exchange of information between services and MA, including the use of SFC web services.

Member State	Response
NL	In cooperation with different intern department which collect and combine information
FR	x
BE	ERDF, JTF and RRF at the SPW: All projects are fed into ARACHNE, and this is going to be done on a quarterly basis. ARACHNE is able to calculate a wide range of risk indicators as long as certain external or internal data is input. The external data comes from the World Compliance and Orbis databases, while the internal data is taken from an XLS file converted to XML (the format required by ARACHNE) and originating from the CALISTA database. The internal data is selected on the basis of the information required by ARACHNE for the ERDF OP. The Excel file generated by CALISTA is based on the file proposed by the Commission on ARACHNE (see Excel Arachne-XMLGenerator). It should be noted that the types of data to be input might change over time in line with any developments to ARACHNE or CALISTA.
AT	Upload from the IDEA database in ARACHNE
SI	Financial Administration of the Republic of Slovenia: As mentioned above the interoperability is achieved between our data analysis tools and databases through direct access. In further steps, the databases are connected with different unique keys among data sources and become a part of the whole specific applications for further IT treatment (calculations, grouping for particular dimensions...). Finally, the data are clearly dynamic analysed and presented as state-of-play, graphs, tables, reports, trends, clusters, etc. In this way, the suspicion patterns, economic operators, or transaction can be identified quickly and easily.
CZ	Automated downloading of data from the Commercial and Insolvency Register into the State Agricultural Intervention Fund information system. This involves interfaces with external systems (the ESM information system and MS2021+, ARACHNE and MS2021+). A single search tool; data segment sharing between systems, internal data warehouse (in-house data).
HU	The EUPR and FAIR system has a fraud prevention function, the use of which is an integral part of our workflow. We also use a number of external databases.
SK	The ITMS21+ system provides and will provide an online interface for the availability of machine-processable data recorded in the system, which are fully available for interoperability with any information system. The following systems are currently integrated in ITMS21+: ISUF, Register of addresses, Register of legal entities, Register of natural persons, Register of public sector partners, National Labor Inspectorate, Register of bankrupts, Tax administration (e.g. information on tax arrears), Register of accounting financial statements, Health Insurance Company, Social Insurance Company. The integration of the criminal record system and EVO (Electronic Public Procurement) is still being prepared. Data exchange takes place through the standardized REST and SOAP protocols. These systems are connected to ITMS21+ mainly for the purpose of obtaining and verifying data, such as information on legal entities, real estate ownership, or information on health and social insurance. For Slovak RRF works the secured storage for the database in the government cloud and their application communicates via API connection. The module is under development but based on API.
PL	For example, in one of the national IT tools, the 'Cross-checks' (Kontrole Krzyżowe) application, the data analysis concerns financial documents (invoices and documents with equivalent probative

Member State	Response
	value) contained in the 'Projects' (Projekty) application, which is also part of the central IT system CST2021. The algorithm generates correlated invoice groups (Grupy Faktur Skorelowanych, GFS) when it identifies that the same financial document, with the same issuer identifier and date of issue, appears several times in payment applications in at least two different projects, and the sum of eligible expenditure from the documents constituting the correlated invoice group exceeds the highest gross amount indicated in these documents. The system defines correlated invoice groups containing groups of settlement documents recognised by the system as invoices requiring cross-checking. Each group is established on the basis of a score resulting from model rules indicating the likelihood of double funding. The overall score consists of 6 main components, where each component score seeks to assess and detect irregularities using a different method.
MT	Our centralized information system supports interoperability through multiple mechanisms. It generates reports in Excel or XML format, ensuring compliance with the requirements of relevant national authorities. Additionally, the system integrates various internal and external APIs to minimize manual data entry and enhance data validation and verification at the point of entry. For more specific needs, ad hoc reports can be developed with the support of the information system development team.
EE	The grants information system has several interfaces with various national registers, enabling certain data to be automatically retrieved/used and verified. For example, control of the Business Register, the Public Procurement Register and the Punishment Register data.
RO	<ul style="list-style-type: none"> <li>- The Ministry of Energy: By consulting platforms dedicated to the call for projects, or those which manage information applied concerning State aid</li> <li>- REGAS or risk management - ARACHNE, the real beneficiary - ONRC, the irregularity advisers facilitate the process of understanding how to make use of the information received and/or obtained in order to validate or invalidate the suspicion of irregularity.</li> <li>- ADR VEST: Using XML files</li> <li>- North-West Regional Development Agency (ADR NORD-VEST): Interoperability is achieved through APIs. (There is currently interoperability between our internal database and MySMIS2021).</li> <li>- The CENTRE Regional Development Agency - The RECOM database of the Trade Register Office is integrated into MySMIS 2021.</li> <li>- MDLPA: Jems Architecture components, Jems Web/Application server, MariaDB- database storage, MinIO</li> <li>- file storage, Elastic Search - system logging (Details available at: <a href="https://jems.scrollhelp.site/manual/v12 /system-architecture">https://jems.scrollhelp.site/manual/v12 /system-architecture</a>)</li> <li>- MIPE - DGMMRR: Interconnection of existing platforms at Ministry of Finance level, ONRC, MIPE-SMIS</li> </ul>
PT	Interoperability is achieved through the integration platform and the data platform, where the data is stored and managed. The technological architecture allows data from different sources to be integrated into an automated and orchestrated standardised process, and the model implemented supports different databases, files and APIs.
IT	As already stated, the Integrated Anti-Fraud Platform (PIAF-IT) was developed, and cofinanced by the European Commission (OLAF) with Hercule III funding, in order to strengthen risk analysis in



Member State	Response
	<p>the management of EU funds. Specifically, it is an IT tool that extracts, aggregates and reconciles data from national and EU sources to generate factsheets on natural or legal persons.</p> <p>The platform is used as an effective tool supporting Arachne with the aim of consolidating and strengthening the fight against irregularities, fraud and other illegal activities against the EU budget both before expenditure is certified and during the ex-post control stage, as well as during administrative checks on implementation of the National Recovery and Resilience Plan.</p> <p>PIAF-IT has recently been upgraded to improve its reporting functionalities and thus provide new information and an improved user experience. In particular, the platform has been connected to new databases to improve the information content of the modules and provide more complete and detailed information to be used during the assessment process, with the additional information coming from increased interoperability.</p>

Q.2.14 Does your digitalisation strategy prioritize the standardized use of digital tools and technologies across local levels and different administrations so that all authorities involved in the anti-fraud strategy can access it?

Response	Frequency	Percentage	Member States
Not applicable (unable to provide an evaluation)	9	33.3%	IE, HR, SE, EL, AT, FI, CZ, ES, HU
Yes, standardization of digital tools is a central goal of our strategy	6	22.2%	FR, BE, SK, MT, PT, IT
Other (please specify)	4	14.8%	LU, SI, PL, EE
No, but we are planning to focus on standardization in future initiatives	3	11.1%	NL, BG, RO
Standardization is not considered essential in our digitalisation efforts	3	11.1%	LT, DE, DK
We are currently assessing the benefits of standardizing digital tools	2	7.4%	CY, LV

Following Q.2.14, please specify "Other".

Member State	Response
LU	We are planning to focus on standardization in future initiatives. Note that the first answer is also applicable.
SI	Financial Administration of the Republic of Slovenia (FARS) answers YES standardization of digital tools is a central goal of our strategy and in addition FARS explains: We evaluate totally

Member State	Response
	successful implementation of the digital tools at different administrative levels in FARS, but we cannot evaluate this topic at different administrative levels outside FARS.
PL	The managing authorities of all cohesion policy programmes are required to draw up their own document on how to prevent and deal with corruption and fraud, including conflicts of interest in the respective programme (the document must also include information on the digitalisation of the fight against fraud). Regardless of the level of administration, the competent ministry ensures access to digital tools and technologies designed for the purpose of fighting fraud. However, it is up to the managing authority to decide how these tools are used. The aim is to ensure the most effective use of tools in the process of combatting fraud at programme level. The tools developed by the EC/OLAF (mainly IMS) are an exception, and they are used by the institutions in a standardised manner, resulting from the relevant EU regulations and national procedure.
EE	Estonia's digitalization strategy can be called the "Digital Society Development Plan 2030" (DAK), and to implement it, each ministry prepares an ICT strategy for its own field. The DAK does not contain sectoral digitalization goals, and these should be included in the ICT strategy of the MoF, which is not a public document.

#### Q.2.15 How do you evaluate the successful implementation of the digital tools at different administrative levels?

Response	Frequency	Percentage	Member States
Partially successful	16	59.3%	SE, NL, FR, EL, BE, AT, FI, LT, SI, ES, SK, BG, EE, PT, LV, DK
Other (please specify)	6	22.2%	IE, LU, HR, CZ, DE, RO
Totally successful	4	14.8%	HU, PL, MT, IT
Not successful	1	3.7%	CY

Following Q.2.15, please specify "Other".

Member State	Response
IE	n/a
LU	We are planning to focus on standardization in future initiatives.
HR	Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development is planning to implement of the digital tools at their administrative levels.

Member State	Response
CZ	No such evaluation has taken place.
DE	The Bremen ERDF Managing Authority: Digitalisation is constantly being developed. The Schleswig-Holstein ERDF Managing Authority: Partially successful
RO	AFIR: Insufficient data taken over from ARACHNE existing in Romania.

Q.2.16 To what extent have digital tools been spread and adopted across different administrative levels?

Response	Frequency	Percentage	Member States
Not applicable (unable to provide an evaluation)	13	48.1%	IE, HR, SE, BE, AT, FI, LT, SI, CZ, ES, BG, CY, EE
Achieved dissemination to all administrative levels	10	37.0%	NL, EL, HU, SK, DE, MT, RO, PT, LV, IT
Other (please specify)	4	14.8%	LU, FR, EL, PL
Limited dissemination to specific regions/localities only (please specify)	1	3.7%	DK

Following Q.2.16, please specify "Limited dissemination to specific regions/localities only".

Member State	Response
DK	The Danish Business Authority: The managing authority makes use of an external auditor, that, in order to carry out audits on all projects has been granted access to the reporting system of the managing authority.

Following Q.2.16, please specify "Other".

Response	Frequency	Percentage	Member States
Digitalisation concerns procedures in general and not specifically fraud.	1	3.7%	EL
The institutions of the system for the implementation, management and control of cohesion policy at different levels have the appropriate digital tools at	1	3.7%	PL

Response	Frequency	Percentage	Member States
their disposal to fight fraud. Access to those tools has been ensured by the Institution Coordinating the Partnership Agreement. In addition, some institutions have their own anti-fraud tools that they have created or purchased themselves.			
Use of external tools and frequent exchange of information. Dissemination successfully achieved to key stakeholders.	1	3.7%	LU
x	1	3.7%	FR

**Q.2.17 What are the key challenges you face in accelerating the digitalisation of your fight against fraud?**

Response	Frequency	Percentage	Member States
Data privacy and security concerns	19	70.4%	IE, SE, NL, EL, BE, AT, FI, SI, CZ, ES, HU, SK, PL, DE, EE, RO, PT, DK, IT
Legal or regulatory barriers	19	70.4%	IE, HR, SE, NL, EL, BE, FI, SI, CZ, ES, PL, DE, BG, MT, CY, EE, RO, LV, IT
Budget limitations	17	63.0%	LU, HR, NL, EL, BE, FI, SI, CZ, ES, HU, SK, PL, DE, BG, EE, RO, LV
Integration challenges with legacy systems	17	63.0%	IE, LU, HR, NL, EL, BE, SI, ES, SK, PL, DE, BG, EE, RO, LV, DK, IT
Lack of expertise	15	55.6%	LU, HR, NL, EL, BE, FI, SI, CZ, ES, HU, SK, DE, BG, RO, PT

Response	Frequency	Percentage	Member States
Resistance to change	9	33.3%	LU, HR, EL, CZ, ES, BG, CY, RO, LV
Accessibility at a regional / local administration level	8	29.6%	IE, HR, EL, BE, CZ, CY, RO, DK
Other (Please specify)	3	11.1%	SI, DE, RO

Following Q.2.16, please specify "Other".

Member State	Response
SI	Financial Administration of the Republic of Slovenia answer: We believe that the key challenges we face in accelerating the digitalisation of our fight against fraud are the access of data different - additional sources, data integration and data conformability (unique structures) and also data privacy and security concerns. Furthermore, we believe that the lack of advanced IT experts, developers and analytics remains the most important issue in public sector. Nevertheless, the lack of human resources could be also one of the challenges, which we face with.
DE	The Bremen ERDF Managing Authority: Conceptual preparatory work still to be done.
RO	AFIR: ARACHNE

Q.2.18 Has your Member State conducted evaluations to assess the interoperability of national systems with Arachne?

Response	Frequency	Percentage	Member States
Not applicable (system already used)	10	37.0%	FR, EL, BE, AT, HU, SK, BG, MT, LV, IT
YES	10	37.0%	LU, SE, FI, CZ, ES, PL, CY, RO, PT, DK
NO	6	22.2%	IE, HR, NL, SI, DE, EE

Q.2.19 If “YES” to Q.18, Please provide key findings or the stage of completion concerning system interoperability.

Member State	Response
LU	One stakeholder reports difficulties in connecting ARACHNE with their systems. The administrative effort is very high and not sensible in terms of costs/benefits.
SE	As part of a public inquiry (SOU 2024:22 A new way to organise the management of EU funds), the Swedish government has examined the need for a common digital platform. The inquiry concludes that Arachne should be used, but that it is necessary to analyse more carefully whether the system is compatible with Swedish legislation on public access and secrecy. To this end, the Government has launched a new inquiry (Use of certain tools to protect the Union’s financial interests - Regeringen.se). The purpose of this inquiry is to ensure that data is entered in accordance with Swedish legislation and to analyse whether using Arachne for purposes other than data entry is compatible with Swedish legislation.
FI	Exploratory work in relation to certain EU funds is still ongoing.
CZ	<p>As part of the pre-analysis so far, the Directorate-General for Finance has focused on the interoperability of systems, i.e. the possibility of using ARACHNE as an integrated preventive technology tool provided by the European Commission as part of its process of developing control plans, data mining and risk identification. The ARACHNE tool aims to make it easier for staff to check specific activities and to develop a control plan with the best possible targeting of checks on structural funds, specifically the European Social Fund (ESF) and the European Regional Development Fund (ERDF).</p> <p>1. Basic key findings: Incorporation of ARACHNE into the process of developing control plans: ARACHNE is expected to enable more effective identification of risk areas and contribute to better targeting of control mechanisms. The integration of these data into the analytical processes of the Financial Administration will strengthen the prevention and detection of possible irregularities in project funding. Interconnection of available data from other sources (State Treasury, Subsidies Register - ReD information system, Model - Risk Indicator Set - Subsidies) and information from ARACHNE: To prepare a model that is directly linked to the outputs of the subsidy data publication working group (PSPDD), i.e. the expected transfer of subsidy data from the State Treasury (for a certain period from the ReD information system), where it is expected that these data will be supplemented with information from ARACHNE in the future. It is expected that, in order to identify projects, recipients of public contracts and suppliers with a higher likelihood of fraud, conflict of interest and other irregularities, the individual pieces of information will be linked with the already existing Model – Risk Indicator Set – Subsidies.</p> <p>2. Completion phase: The Subsidy Risk Coordinators Working Group (KONDOR) is testing the ARACHNE tool, i.e. the possibility of using the information presented here for the development of control plans. At the Directorate-General for Finance, testing is underway on exporting data from ARACHNE and subsequently linking them to other data sources, specifically the ReD information system and Model – Risk Indicator Set – Subsidies. Both areas are in the initial phase of testing, which is expected to be completed by the end of 2025.</p>

Member State	Response
	One of the managing authorities indicated that the data reported in Arachne are different from those in the national systems and registers.
ES	Work is underway to adapt the FEAGA paying agency's management applications to generate upload files in Arachne with the necessary information for a useful risk analysis.
PL	<p>In the area of cohesion policy, an assessment was carried out of the interoperability of the national systems with the Arachne tool. The analysis was performed on the available documentation for Arachne. A comparative analysis of the functionality of the national IT tools with Arachne was also carried out in terms of the rationale behind creating applications, risk analysis, the impact of users on risk analysis, changes in risk analysis parameters, application type, data origin, scope of data, integration with additional databases, additional administrative burden, detection of irregularities, 'economic intelligence' functions, use of AI. The analysis showed that Arachne, in its current form, is not fully suited to the needs of the institutions. Some flaws in the functions of the tool and difficulties in using it were identified, including but not limited to the presence of false positive results, legal barriers, in particular as regards compliance with national data protection rules, additional administrative burden related to the collection of data for Arachne, unclear algorithms for the calculation of individual risk indicators, lack of an error-handling tool.</p> <p>In addition, Arachne is currently used as part of the National Recovery and Resilience Plan, including the cyclical transmission of input data.</p>
CY	System interoperability at the moment is not possible. We can feed data to Arachne. At the moment we are planning to upload back to our MIS data from Arachne through an XML file.
RO	Ministry of Energy: The ARACHNE system is implemented at DGI-ME level and is consulted in order to obtain information on how to effectively manage irregularities.
PT	At present, Fund data is integrated by uploading an XML file to the ARACHNE platform. The intention is that this reporting is done by means of interoperability in the future. Considering that the process of implementing interoperability is in the phase where the specifications of the services provided by the ARACHNE platform are being analysed, it is not yet possible to draw conclusions on this topic at this stage.
DK	Most of the contributions to the survey reported a "No" in Q.2.18. The Danish Agency for Green Land Conversion and Water Environment reported "Yes" and noted: We are at a very early stage in our evaluations.

**Q.2.20** What steps have you undertaken to ensure your systems are prepared to feed data into Arachne for the upcoming multiannual financial framework? Please refer to the indicative milestones from figure 1 and select the ones you have reached.

Response	Frequency	Percentage	Member States
Data identification: Identified data sources	11	40.7%	HR, BE, ES, SK, BG, CY, EE, RO, PT, LV, IT



Response	Frequency	Percentage	Member States
Scoping/Assessment: Assessed technical and operational requirements	10	37.0%	LU, BE, ES, SK, PL, CY, EE, RO, DK, IT
No preparation actions taken in 2024	9	33.3%	IE, HR, NL, FR, EL, FI, LT, SI, DE
Other (please specify)	9	33.3%	HR, SE, CZ, ES, SK, PL, MT, CY, RO
Data Mapping: Mapped the data (ensured that the data and system structure are compatible with Arachne's system)	8	29.6%	HR, BE, AT, SK, CY, EE, RO, PT
Testing: Conducted tests to confirm system's capability to feed data	7	25.9%	BE, SI, CY, EE, RO, LV, IT
Development /Adjustment: Started or completed necessary system modifications	6	22.2%	BE, ES, SK, CY, EE, RO
Planning: Developed detailed plans for integration	5	18.5%	BE, ES, EE, RO, IT
Resource Allocation: Allocated necessary budget and human resources	5	18.5%	BE, ES, CY, EE, RO
Completed Integration: Successfully integrated systems with Arachne	3	11.1%	BE, HU, BG

Following Q.2.20, please specify "Other ".

Member State	Response
HR	Our Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development highlighted the following answers: Data identification: Identified data sources and Data Mapping: Mapped the data (ensured that the data and system structure are compatible with Arachne's system)
SE	An inquiry has been launched to ensure that the legal conditions will be in place.
CZ	Given the connection of the MS2021+ national information system to Arachne and the data sharing that is already set up and fully operational, it is not considered necessary to further modify this area.
ES	The answers provided to Q2.20 refer only to one authority. The other authorities' answer was No preparation actions taken in 2024

Member State	Response
SK	The RRF is preparing automation of data export for API integration on Arachne. The process of API integration has already been discussed with the Arachne support team in the European Commission.
PL	Arachne is currently used as part of the National Recovery and Resilience Plan, including the cyclical transmission of the input data.
MT	The process to upload data on Arachne starts with the extraction of xml files from the national management information systems. Prior to uploading, these files are validated on the Arachne database itself to check whether the xml text contains any errors (using the Data Upload icon and selecting the field 'File Validation'). If the files are validated successfully, these files are uploaded on Arachne (using the Data Upload icon and selecting the field 'File Upload'). The database prompts you whether the files have been uploaded satisfactorily or not.
CY	Arachne is used for Cohesion and Fisheries funds programs and the RRP. Planned to be used for agricultural policy programs and migration programs. Data is imported in Arachne through an XML file.
RO	AFIR: At present, data are entered manually (XML loading). In the first quarter of 2025, we plan to develop software for the automatic uploading of data

**Q.2.21** Currently, what are the factors preventing you from being able to feed the data into Arachne?

Response	Frequency	Percentage	Member States
Not applicable, already using it	18	66.7%	IE, LU, HR, FR, EL, BE, AT, SI, CZ, HU, SK, BG, MT, CY, RO, PT, LV, IT
Technical limitations	7	25.9%	NL, FI, LT, CZ, ES, RO, DK
Uncertainty about tool's effectiveness	7	25.9%	FI, LT, CZ, PL, DE, EE, DK
Budget constraints	5	18.5%	NL, FI, CZ, ES, EE
Lack of staff expertise	5	18.5%	FI, LT, ES, RO, DK
Legal constraints	5	18.5%	SE, NL, FI, ES, DE
Other tool(s) already in use	4	14.8%	CZ, ES, PL, DK

Q.2.22 What type of support would facilitate your successful integration of data into Arachne by the required deadline?

Response	Frequency	Percentage	Member States
Training programs / Information sharing (handbooks etc.)	16	59.3%	HR, NL, AT, FI, LT, SI, CZ, ES, PL, DE, BG, MT, RO, PT, DK, IT
Technical assistance	13	48.1%	HR, NL, FI, LT, CZ, ES, SK, DE, BG, MT, RO, DK, IT
Financial support	10	37.0%	HR, NL, FI, CZ, ES, DE, BG, EE, RO, IT
Not applicable	9	33.3%	IE, LU, FR, EL, BE, SI, HU, CY, LV
Other (please specify)	4	14.8%	SE, PL, MT, EE

Following Q.2.21, please specify "Other".

Member State	Response
SE	Legal support, ensuring timely answers to questions so that Sweden can assess the system's legal implications
PL	<ol style="list-style-type: none"> <li>1. Streamlining the data input process to reduce the administrative burden.</li> <li>2. Strengthening the function allowing users to remove red flags that have already been noticed and assessed as 'clear', i.e. not reflecting real fraud risks, in order to reduce the number of false positive results.</li> <li>3. Providing Member States with details of the risk analysis applied (currently users see only the end result).</li> <li>4. A well-functioning Service Desk where flaws in the functioning of the tool could be reported and followed up until feedback is received confirming or ruling out the flaw.</li> </ol>
MT	Financial support provided by the European Commission.
EE	ARACHNE should be developed to make data analysis broad and useful. Overly general evaluation criteria will not yield results.

Q.2.22 What type of support would facilitate your successful integration of data into Arachne by the required deadline?

Response	Frequency	Percentage	Member States
Training programs / Information sharing (handbooks etc.)	17	63.0%	LU, HR, NL, AT, FI, LT, SI, CZ, ES, PL, DE, BG, MT, RO, PT, DK, IT
Technical assistance	14	51.9%	LU, HR, NL, FI, LT, CZ, ES, SK, DE, BG, MT, RO, DK, IT
Financial support	11	40.7%	LU, HR, NL, FI, CZ, ES, DE, BG, EE, RO, IT
Not applicable	6	22.2%	FR, EL, BE, HU, CY, LV
Other (please specify)	6	22.2%	IE, LU, SE, PL, MT, EE

Following Q.2.22, please specify "Other".

Member State	Response
IE	There is no national anti-fraud strategy in place, so the management of EU funds is devolved so difficult to answer for all, but points raised include the lack of a national id number, and GDPR concerns around data sharing
LU	Customized guidance taking into account the specificities of national programs and the available data (type and formats).
SE	Legal support, ensuring timely answers to questions so that Sweden can assess the system's legal implications
PL	<ol style="list-style-type: none"> <li>1. Streamlining the data input process to reduce the administrative burden.</li> <li>2. Strengthening the function allowing users to remove red flags that have already been noticed and assessed as 'clear', i.e. not reflecting real fraud risks, in order to reduce the number of false positive results.</li> <li>3. Providing Member States with details of the risk analysis applied (currently users see only the end result).</li> <li>4. A well-functioning Service Desk where flaws in the functioning of the tool could be reported and followed up until feedback is received confirming or ruling out the flaw.</li> </ol>
MT	Financial support provided by the European Commission.

Member State	Response
EE	ARACHNE should be developed to make data analysis broad and useful. Overly general evaluation criteria will not yield results.

#### Q.2.23 As part of your anti-fraud strategies, are you considering the use of Arachne?

Response	Frequency	Percentage	Member States
Already in use	18	66.7%	LU, HR, FR, EL, BE, AT, SI, CZ, HU, SK, PL, BG, MT, CY, RO, PT, LV, IT
Undecided	5	18.5%	IE, FI, ES, DE, DK
Planning to use	4	14.8%	SE, NL, LT, EE

#### Q.2.24 If “Already in use” or “planning to use” to Q.2.21, please elaborate on your (planned) use of the tool. If “No plans to use”, please provide a brief explanation for not planning to use Arachne.

Member State	Response
LU	<p>The use of ARACHNE is primarily limited to the import of our data into the ARACHNE system.</p> <p>NB: One stakeholder reports that they have no plans to use it.</p>
HR	<p>Contribution from Ministry of Labour, Pension System, Family and Social Policy, Directorate for the Management of EU:</p> <p>Arachne is a mandatory tool for fraud detection in the ESF procedural rules.</p> <p>Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development has detected two risk indicators to track, “Beneficiaries involved in multiple Ops” and “Links between beneficiaries and contractors” which they will try to use to detect potential cases of undisclosed double financing and conflict of interest between beneficiaries and contractors. The projects with high score on these indicators are checked more thoroughly.</p>
SE	<p>Sweden intends to comply with the requirements of the Financial Regulation. Sweden also sees benefits in using the system more extensively also for ex ante controls to ensure that double funding and conflicts of interest do not occur. However, such use must be compatible with the Swedish Public Access to Information and Secrecy Act, and this is currently being investigated.</p>
NL	<p>Planning to use new Arachne</p>

Member State	Response
FR	<p>Not all the bodies that manage cohesion policy funds use Arachne. Arachne enables the management bodies that use it to bolster their procedures for the prevention and detection of risks of irregularities or fraud.</p> <p>However, it also increases the administrative burden on the staff responsible for management checks. Arachne contains an array of information that makes it difficult to understand, with risk indicators that are difficult to interpret. The risks that the system can highlight are not always relevant or of a scale proportionate to the control and management of financial transactions funded by the cohesion policy.</p> <p>The management bodies also use various databases which can be consulted instead of or as well as Arachne (Manageo, Fiben, Societe.com, Infogreffe, Diane, Pappers, API entreprise, etc.). The consultation of digital tools or information systems for data on beneficiaries of EU funds is integrated into all the managing authorities' management verification procedures and anti-fraud measures.</p> <p>In other areas, in line with the recommendations of the European Commission, consulting Arachne is one of the means to detect fraudulent practices as decided upon by the management bodies of the YEI and ESF national operating programmes for the 2014-2020 programming period.</p> <p>As far as the CAP is concerned, the paying agencies have not begun to use Arachne at this stage. Work is under way to gain familiarity with how the tool works and to anticipate with DG AGRI and the paying agencies any adaptations of the system that might be necessary to the specificities of the CAP.</p>
EL	<p>Recovery and Resilience Facility Coordination Agency (RRFA): The tool is used for the ex-ante control of absence of conflict of interest in public procurement and loan contracts.</p>
BE	<p>ERDF, JTF and RRF at the SPW: All projects are fed into ARACHNE, and this is going to be done on a quarterly basis. ARACHNE is able to calculate a wide range of risk indicators as long as certain external or internal data is input. The external data comes from the World Compliance and Orbis databases, while the internal data is taken from an XLS file converted to XML (the format required by ARACHNE) and originating from the CALISTA database. The internal data is selected on the basis of the information required by ARACHNE for the ERDF OP. The Excel file generated by CALISTA is based on the file proposed by the Commission on ARACHNE (see Excel Arachne-XMLGenerator)</p>
AT	<p>No information.</p>
LT	<p>MoF currently awaits for training from the EC on Arachne. After the training we will carry out a trial to evaluate how long does it take to update data in Arachne and will start required actions to adapt our national IT system for ESIF and RRF to Arachne.</p>
SI	<p>Arachne is already in use and will continue to be used for management verifications. We also provide users with training on how to use the tool. Note: Arachne is used by the Managing Authority, the Intermediate Body, the Implementing Body and the Audit Authority</p>
CZ	<p>Evaluation of projects/applicants and subsequently beneficiaries; one of the bases for risk analysis; monitoring the connections between ownership structures, checking conflicts of interest under Article 61 of the Financial Regulation (in particular, checking conflicts of interest with the implementation structure and conflict of interest in public procurement), checking sanctions lists and double funding in relation to the project being checked;</p>

Member State	Response
	<p>one of several different tools used to identify the risk of, in particular, conflicts of interest, fraud or double funding; there is a strong emphasis on inputting new data into the tool, but the priority is no longer to update data, including deleting outdated or false data (e.g. when a project is supported first from Programme A, then the subsidy is withdrawn and the same project is supported from another programme. As a result, there may be two identical projects financed from different sources in Arachne, which is not the case, because support was actually provided only from programme B). We consider that both technical and financial assistance from the EC is necessary to ensure satisfactory functionality and increased use of the tool.</p> <p>Use in the control process. Extending the functionalities to include improvements in the ex-ante evaluation or checks of whether the entity being inspected is subject to the application of the sanction Regulations would be very welcome. use in particular in relation to: — evaluating the aid application and issuing the legal act; — administrative verification; — on-the-spot checks.</p> <p>The risk coordinator coordinates the use of Arachne within the OP implementation structure. They keep record of the findings of the verifications of the entities before issuing the legal act and during administrative verification, and subsequently take these findings into account when developing the risk analysis of the projects for drawing up the plan for the on-the-spot checks.</p> <p>Based on the annual risk analysis that is the basis for establishing the on-the-spot check plan, when performing public procurement checks using public registers and Arachne to check potential conflicts of interest, the managing authority carries out regular data and information analyses across operations in order to identify and subsequently carry out a more thorough follow-up of operations showing fraud indicators (e.g. by means of an on-the-spot check). The managing authority is required to use these identified and evaluated data for its control activities, i.e. in particular to identify operations with an increased risk of fraud; verification of the risk of fraud, possible conflict of interest, for example, in the case of persons acting on behalf of tenderers for tenders ranked in the first three places in the selection/tendering procedure, checks are made on connections between the selected contractors and the contracting authority and other possible links, duplication in projects, insolvency and other risk situations; use for ex ante analyses.</p> <p>One managing authority uses the system only marginally because it does not contain, for example, regional subsidies and is therefore not very useful for the authority.</p>
HU	<p>Data specified in EU legislation are uploaded to ARACHNE every 2 months. Applying ARACHNE and documenting the application is generally an integral part of development policy processes. A methodology for the application of ARACHNE and the use of its results has been developed. The methodology will be reviewed annually.</p>
SK	<p>The Arachne tool functions as a compulsory auxiliary search tool of the data contained in it for cohesion policy, in order to identify projects that could potentially be susceptible to fraud risks, conflicts of interest and irregularities. MA/IB primarily try to use the Arachne tool in the project approval phase as well to verify conflicts of interest as one of the possible verification tools. The Arachne tool is also used in implementation phase of projects (payment claims, on the spot checks). Arachne is used by the audit authority as a tool in the performance of audits. Slovak RRP: The line ministries as implementing bodies already use Arachne. The coordinating body (National Implementation and Coordination Authority – NICA) collects all the data on the implementation of the RRP; these are then exported to xml file and uploaded to Arachne on a monthly basis.</p>
PL	<p>Arachne is currently used as part of the National Recovery and Resilience Plan, including the cyclical transmission of the input data. The Institutions responsible for investments have developed</p>

Member State	Response
	<p>procedures that take account of the use of Arachne in the control process. In the case of cohesion policy programmes, since documents concerning anti-fraud measures are drawn up at programme level, individual managing authorities have discretion in this regard.</p> <p>At the Paying Agency, the Arachne system is used, among other things, for the verification of personal and capital links between entities in the context of applications for co-financing of projects or for the disbursement of support. In the course of the checks, the control staff establish the facts and compare them with the state of affairs as required by the rules, procedures and interpretations of the procedures. The use of Arachne as a tool for data acquisition and risk assessment in the context of the NRRP supplements the existing management and control systems used in carrying out verification and control activities and serves to strengthen the control systems, including fraud prevention, avoidance of conflicts of interest and double funding and their detection, and it possibly serves to reduce the rate of occurrence of serious irregularities.</p>
BG	<ul style="list-style-type: none"> <li>- Check for presence or absence of conflict of interest of the composition of evaluation commissions: Carrying out a Check for the presence or absence of a Conflict of Interest, according to Art. 61 of Regulation (EU, Euratom) No. 2018/1046 of the European Parliament and of the Council of July 18, 2018, presence of connectivity within the meaning of § 1, item 9 of the DR of the ZPK and hierarchical dependence of the proposed composition of the evaluation commission. The verification is performed by extracting data from the ARAHNE.</li> <li>- Using the ARAHNE for fraud risk assessment: After completion of an evaluation procedure through the selection of project proposals submitted by private legal entities or non-profit legal entities, before a decision for the grant is made by the Head of the MA, a check is made in the ARAHNE for the presence of a risk of fraud and suspected conflicts of interest. The reference is made on the basis of the information available in ISUN about the submitted project proposals.</li> <li>- Conducting an inquiry in the ARAHNE for the presence of fraud risk and suspected conflict of interest, in the event of a reported irregularity when identifying indicators of fraud ("red flags"). The inquiry is conducted by an employee of the "Irregularities" department."</li> </ul>
MT	<p>As stated in Q.2.18 and Q2.20, Arachne is already in use. The menu 'entity search' is used to check the extent of risk of specific projects, contracts, companies and persons. There are seven risk categories, namely procurement, contract management, eligibility, performance, concentration, reasonability, and reputational and fraud. Each of these 7 risk categories are further subdivided into risk indicators (more than 100). The level of risk and sub-risks of these 7 categories are monitored for any red flags that may ensue in relation to projects and/or contracts, e.g. (1) a high 'reputational and fraud risk' would feature a red flag of potential conflict of interest in relation to the entity in question; and (2) a high 'concentration risk' would feature a red flag of potential double funding in relation to a contract. A high risk would trigger further work outside Arachne to determine whether the red flags translate in actual irregularities/fraud.</p>
CY	<p>Already using it.</p>
EE	<p>The first mapping of our specific needs has been completed. We found that Arachne, on its own, does not help in identifying the specific risks associated with funding measures. Regardless of whether or how extensively Arachne is used, a specific risk assessment based on the measure itself is still necessary. However, Arachne could serve as a supportive tool alongside other administrative control.</p>
LV	<p>Evaluation of risk indicators. Identification of risk signs. Evaluation of inter-company relationships.</p>



#### Q.2.25 Has your Member State implemented ARACHNE?

Response	Frequency	Percentage	Member States
YES	22	81.5%	IE, LU, HR, FR, EL, BE, AT, LT, SI, CZ, ES, HU, SK, PL, BG, MT, CY, EE, RO, PT, LV, IT
NO	5	18.5%	SE, NL, FI, DE, DK

#### Q.2.26 If “YES” to Q.2.25, please specify the entities or individuals that have access to the Member State's data within the Arachne system.

Response	Frequency	Percentage	Member States
Audit authorities	18	66.7%	LU, HR, EL, BE, AT, LT, SI, CZ, ES, HU, SK, PL, BG, MT, RO, PT, LV, IT
Only managing authorities	15	55.6%	HR, FR, EL, BE, AT, LT, CZ, HU, SK, BG, MT, EE, PT, LV, IT
Other (please specify)	12	44.4%	LU, HR, CZ, ES, HU, SK, PL, CY, EE, RO, LV, IT
AFCOS	9	33.3%	BE, LT, CZ, ES, SK, BG, EE, PT, LV
Law enforcement	2	7.4%	LT, LV
Not applicable	1	3.7%	IE

#### Following Q.2.26, please specify "Other ".

Member State	Response
LU	Managing Authorities

Member State	Response
HR	Intermediate Bodies
CZ	Implementation entities in the National Recovery Plan (component owners = managing authorities), inspection officers, intermediate bodies.
ES	Managing authorities
HU	Directorate for Internal Audit and Integrity, Central Coordination
SK	Slovak RRF implementing bodies (line ministries), coordinating body (NICA) and CA (the certifying authority).
PL	Institutions of the National Recovery and Resilience Plan
CY	Treasury of the Republic under its competence to perform controls on behalf of the authorities managing the EU Funds.
EE	Implementing Agencies
RO	MANAGEMENT AUTHORITIES
LV	Paying agency for EU funds for agricultural and rural development, Accounting Body of the ESF, ERDF and CF, Procurement Monitoring Bureau

Q.2.27 If “YES” to Q.2.25, what is the tool used for?

Response	Frequency	Percentage	Member States
Detection	21	77.8%	LU, HR, FR, EL, BE, AT, LT, SI, CZ, ES, HU, SK, PL, BG, MT, CY, EE, RO, PT, LV, IT
Prevention	19	70.4%	LU, HR, FR, EL, BE, AT, LT, SI, CZ, HU, SK, PL, BG, CY, EE, RO, PT, LV, IT
Investigation	12	44.4%	LU, HR, BE, LT, CZ, ES, PL, MT, CY, RO, LV, IT
Not applicable	1	3.7%	IE

Q.2.28 If “YES” to Q.2.25, since implementing it, how has it impacted the efficiency and effectiveness of your anti-fraud efforts?

Response	Frequency	Percentage	Member States
Moderately improved	8	29.6%	BE, AT, CZ, ES, SK, MT, RO, PT
No significant change	6	22.2%	LU, SI, HU, PL, EE, LV
No evaluation was conducted	5	18.5%	IE, HR, FR, LT, BG
Significantly improved	3	11.1%	EL, CY, IT

Q.2.29 If “YES” to Q.2.25, what specific functionalities of Arachne have proven most effective in your state’s fight against fraud?

Response	Frequency	Percentage	Member States
Risk scoring and profiling	15	55.6%	HR, EL, BE, AT, SI, CZ, HU, SK, BG, MT, CY, RO, PT, LV, IT
Pattern detection through data mining	9	33.3%	HR, SI, CZ, SK, BG, CY, RO, PT, IT
Reporting and analytics for supporting investigations	5	18.5%	LU, CZ, ES, CY, RO
Not applicable	4	14.8%	IE, FR, LT, EE
Other (please specify)	4	14.8%	EL, CZ, PL, MT
Automated alerts for irregular activities	3	11.1%	HR, BG, RO

Following Q.2.29, please specify "Other ".

Member State	Response
EL	Recovery and Resilience Facility Coordination Agency (RRFA): The tool is used for the ex-ante control of absence of conflict of interest in public procurement and loan contracts.
CZ	Inspection of projects (entities); searching for companies with a link to owners and managers, as well as searching and sorting by project; identifying ownership structure using ORBIS data;

Member State	Response
	establishing links between high-risk entities; checking links between stakeholders, as a tool for fraud prevention and detection.
PL	Access to data from other Member States provided by institutions based abroad.
MT	With reference to Q2.28, it is to be noted that, to date, the potential benefits ensuing from Arachne are still not being exploited to the full. Once Arachne will be made use of to the full depending on Malta's exigencies, the efficiency and effectiveness of our anti-fraud efforts will be expected to improve significantly.

Q.2.30 If “YES” to Q.2.25, are there procedures in place to address risk alerts generated by the Arachne system?

Response	Frequency	Percentage	Member States
YES	18	66.7%	LU, HR, FR, EL, BE, AT, SI, CZ, HU, SK, PL, BG, MT, CY, RO, PT, LV, IT
NO	3	11.1%	IE, ES, EE
Not applicable	1	3.7%	LT

Q.2.31 If “YES” to Q.2.25, does your system have dedicated resources or a task force for handling the outputs and alerts generated by Arachne?

Response	Frequency	Percentage	Member States
YES	11	40.7%	LU, EL, BE, CZ, ES, SK, PL, MT, CY, LV, IT
NO	5	18.5%	IE, HR, LT, HU, PT
In planning	3	11.1%	BG, EE, RO
Not applicable	3	11.1%	FR, AT, SI

Q.2.32 Please feel free to share any additional thoughts or experiences you have regarding the topics discussed in this section.

Member State	Response
HR	The Audit Authority would appreciate to receive more training and on-the-job practical experience.
NL	N/a, as mentioned the planning is to use New Arachne
FR	Since 2023, the MICAF (France's AFCOS) has had a unit monitoring fraud involving funding for government aid. The unit is tasked, with the support of the investigative, administrative and judicial bodies and the judicial authorities concerned, with mapping aid mechanisms, helping in evaluating their vulnerabilities, sharing best practices, supporting the rollout of filters and blocking mechanisms before government aid is paid unduly, alerting the ministries involved of the risks and of identified fraudulent ventures, enabling the same ministries to analyse them and putting into place the necessary synergy for a collective response to fraud by those ministries.
EL	In specific question fields (e.g. QUESTION 2.9) further clarification could be given for the concepts/definitions listed in the questions (e.g. the concept/definition of 'Data Analysis tools (external)'). This concept/definition covers several fields and there is a risk that the Member States might give a response concerning only one of those fields.
BE	At this stage, the fact that it is necessary to have XML data export tools that can be read by ARACHNE and that no web is service available.
AT	No information.
CZ	<p>(1) The current Arachne system has the following limitations:</p> <p>No possibility to search in Arachne retrospectively back to a selected date in history – This functionality would allow the analysis of ownership structures in specific historical periods, which is important for different types of analysis and legal due diligence.</p> <p>Update frequency of Arachne –updating every 3-4 months is not often enough. External data should be updated every month instead of every three months.</p> <p>Flagging-up in ARACHNE of persons/companies in breach of sanctions, including displaying individual shareholders' shares – This element is necessary to ensure compliance and protect against risks associated with subsidising entities on sanctions lists, for example the Russian sanction lists in the context of the aggression in Ukraine.</p> <p>The absence of the above elements means that Member States are forced to use alternative instruments, which in turn leads to inefficient spending of additional funds.</p> <p>2) The usefulness of Arachne is significantly affected by the quantity of input data in it and how up to date it is. Ensuring data transfers from national systems to Arachne is very demanding technically, financially and in terms of human resources. In order to improve the quality of the data contained in it and thereby make the system more useful, the entities providing the data would need to be provided with rather extensive support by the Arachne system administrator in all three areas.</p> <p>3) One of the issues currently being addressed by all Member States is how to set up a control system for sanctioned entities. This is a complex area where the main problem is that managing authorities, such as grant providers or contracting entities, do not have sufficient and appropriate sources of information for high-quality assessment of individual entities. For example, they do not have access to beneficial ownership registers in all Member States, let alone non-EU countries. Or, if they want to obtain access, it is expensive, which is certainly not an efficient use of money. The Arachne tool contains unique information and could be a leader and innovator in this field,</p>

Member State	Response
	<p>providing those entities with information that they can use in their screening and monitoring. Arachne is linked to the Register of Beneficial Owners of the Czech Republic and, we assume, of other Member States too. This, in conjunction with the Orbis and World-check databases and other information contained in Arachne, could provide a basis for such verification. We believe it would be appropriate and possible for this functionality to be added, including the use of this information to identify further links and control pursuant to Articles 5 l and 5k of Regulation 833/2014. Given the plans to make further and more intensive use of Arachne, this could be another reason to convince all Member States of the appropriateness and usefulness of the tool.</p>
ES	<p>Compatibility of management applications with the tool and preparation of files for the tool's feed is a major challenge for paying agencies. Working groups are being set up with paying agencies in other Member States to identify the most useful risk indicators for each population.</p>
HU	<ol style="list-style-type: none"> <li>1. Making bulk exports more flexible in the framework of ARACHNE reports would improve the effectiveness of work to protect the EU's financial interests.</li> <li>2. From a quality assurance point of view, the monitoring of users' activities on the 'Admin' page of the User Management Module is justified.</li> <li>3. For compliance with the GDPR, it is important that individuals' data is automatically concealed when screenshots are taken.</li> <li>4. We need to speed up the creation of conditions for automatic data links between ARACHNE and Member States' monitoring systems (e.g. FAIR in Hungary).</li> <li>5. Detailed and practical information is needed on the intended successor to ARACHNE after 2028.</li> <li>6. The ARACHNE search system needs to be improved upon, as it is difficult to find data and organisations. This has a negative effect on the practical application of ARACHNE and thus threatens the protection of financial interests (e.g. a person entitled to use a program is not able to see alerts based on data uploaded to another programme).</li> <li>7. In the case of false alerts (red flags), the user is unable to indicate the low risk of the alert (e.g. several companies on one site may be standard procedure in a single office building).</li> <li>8. The ARACHNE interface displays indicators in several locations, but there are a number of cases where it is not possible to access the details on the basis of which a given indicator takes its values.</li> </ol>
SK	<p>The Central coordinating body issued the Manual for Arachne version 1.0 for the program period 2021-2027. After several meetings with intermediary bodies, the public procurement office, the Audit authority, we came to conclusions which should make work with the Arachne tool more efficient and also reflect changes, which entails a new analysis of public procurement risks. Outputs and alerts are to be handled by the line ministries in RRF.</p>
PL	<p>None</p>
DE	<p>The Baden-Württemberg ERDF Managing Authority: ARACHNE is not currently used because:</p> <ol style="list-style-type: none"> <li>1. it is disproportionate under German privacy and data protection law since it encroaches on the rights of beneficiaries and their contractual partners;</li> <li>2. it appears to be of little use since it is not able to make nuanced statements about beneficiaries, their legal and procedural compliance, and their social and business relationships; and</li> <li>3. it is unlawful since no authorisation for this kind of data collection and analysis is currently in place.</li> </ol>

Member State	Response
MT	<p>While on-line video tutorials on Arachne Academy are very useful, Malta recommends that the Arachne User Manual be more user-friendly.</p> <p>Malta does actually tackle the risks ensuing from searches on Arachne. To cite an example already described in answer to question Q.2.24, a high ‘reputational and fraud risk’ would feature a red flag of potential conflict of interest in relation to the entity in question, and this is acted upon. Thus, the fact that there are no formal procedures to address risk alerts generated by the Arachne system, this does not imply that Malta is not utilizing the IT Tool’s outputs effectively as, in actual fact, emerging risks are tackled. Moreover, plans are underway to allocate dedicated resources specifically tasked with handling Arachne's outputs and alerts. This proactive approach demonstrates that Malta is committed to leveraging Arachne's capabilities and reflects its dedication to improving risk management and ensuring compliance with EU funding standards.</p>
CY	<p>Arachne is a good tool however a lot more additional work is required in order to further investigate the flags identified in Arachne and corroborate the reality of the flags through other information and databases. Frequently flags raised are not corroborated.</p>
EE	<p>Our ARIB has some slides to introduce their experience.</p> <div> <p><b>Organisation/GoV</b></p> <p>igament and</p> <p>a upload for on 03 April ,</p> <p>is automatic.</p> <p>ne data. The</p> <p>i)</p> <p>67 ex-ante</p> <p>EE_ARIB_ARACHNE_estimated time consumption 2019-</p> </div>



REPUBLIC OF ESTONIA  
AGRICULTURAL REGISTERS  
AND INFORMATION BOARD

## Data uploaded by the PA in

\* Data uploaded by the PA in Arachne => 49 /100+ (mandatory 15/100+)

Metadat fields	Project data	Contracts	Expenses	Entities	Related People	Contract-Service providers
Source	Project ID	Contract ID	Expense ID	Entity ID	First name	Contract ID
Date	Project name	Contractor ID	Project ID	Entity name	Last name	Service Provider ID
Author	Status	Project ID	Contractor ID	Zipcode	Birthday	
Programme/Plan ID	DG	Contract name	Expense type	City	Project ID	
Authority/Agency	Project type	Contract description	Invoice date	Country Code	Function	
Currency	Beneficiary ID	Amount	Payment date			
Member State	Total cost	Valid tenders	Amount			
	Turnover					
	Nbr of employees					
	Start date					
	End date					
	EC financial assistance					
	Other contribution					
	DG					
	Project type					

\* Method of transmission (manual/automatic)

➤ [manual, API integration is under consideration \(IT prioritization and cost estimation process\)](#)

\* Did you have to rebuild your internal IT-systems or do you keep the information that you upload and download in separate IT-systems or IT files?

➤ [Data from IT systems collected and into central SAP BO data warehouse](#)

➤ [SAP BO based report built up, collectst 95% data => manual work: cleaning, format change, upload \(2hrs per upload\)](#)

\* How do you ensure that the data you "feed into" Arachne is correct?

➤ [data quality and integrity are checked during the manual data compilation phase](#)



PT

There is a need to integrate ARACHNE data with the application systems, so, as with the services for the interoperability of data reporting, there should be services for providing ARACHNE data that can be integrated into our systems.

DK

The Danish Business Authority: Uncertainty about the interoperability between the current Arachne and the new one under development is not demanding for a decision to start using Arachne.

### Q.3.1 Have there been any changes in your anti-fraud governance structures in place in 2024?

Response	Frequency	Percentage	Member States
NO, no changes to the existing anti-fraud governance structure were introduced	20	74.1%	IE, HR, SE, FR, EL, BE, AT, FI, LT, SI, CZ, HU, SK, PL, BG, MT, EE, RO, PT, DK
YES, we modified the existing anti-fraud governance structure	6	22.2%	LU, NL, ES, CY, LV, IT
NO, we do not have an existing anti-fraud governance structure	1	3.7%	DE



Q.3.2 If “YES, we set up an anti-fraud governance structure” or “YES, we modified the existing anti-fraud governance structure” to Q.3.1, what are the key changes implemented?

Member State	Response
LU	Analysis and Update of the anti-fraud system.
NL	New Coordination of anti-fraud is set up and placed with AFCOS
ES	<p>The Statute of the Independent Authority for the Protection of Whistleblowers has been approved, a state authority whose purpose is to guarantee the protection of the whistleblower, to serve as an institutional pillar in the prevention and fight against fraud and corruption, and to guarantee the integrity of the administrations and personnel in the service of the public sector.</p> <p>Two similar Independent Whistleblower Protection Authorities have also been created at regional level. One post has been created for an Economic Crimes Chamber Prosecutor and one post for a Public Administration Crimes Chamber Prosecutor, specialising mainly in the fight against public and private corruption, organised crime and gender-based violence.</p> <p>At internal level, some entities have developed anti-fraud structures. For example, The Civil Guard Sustainability Plan 2021-2025 is currently in force. This Plan contemplates five Projection Axes, the first of which is Governance. It contains the following commitments, each of them contemplating two differentiated areas of action:</p> <ul style="list-style-type: none"> <li>- Institutional Governance (two areas both related to Regulatory Footprint).</li> <li>- Human Rights (internal training and awareness-raising; external promotion)</li> <li>- Fight against Corruption (Code of Ethics; Corruption prevention)</li> <li>- Transparency (Management, Public Tendering)</li> <li>- Sustainable Innovation (Green Procurement; Innovation, Innovation)</li> </ul>
CY	The Ministry of Interior in its competence as the managing authority for Home Funds has been added in the anti-fraud governance structure.
LV	New NAFS is approved. Managing Authority of the Social Climate Fund is newly included in our anti-fraud governance structures in 2024.
IT	<p>The Committee for Combatting Fraud against the European Union (COLAF) is the government ‘tool’ charged with drawing up and developing the national strategy for fighting irregularities and fraud against the European Union budget and for ensuring cooperation and coordination between all of the national administrations with roles of various types in this area, and also between those administrations and the competent Commission departments. COLAF has been designated as the ‘Anti-fraud coordination service’ (AFCOS) pursuant to Article 12a of Regulation (EU, Euratom) No 883/2013 and is thus responsible for facilitating cooperation and information exchange with OLAF, including of an operational nature, and for drawing up the national anti-fraud strategy.</p> <p>In 2024, Article 3 of Decree-Law No 19 of 2 March 2024 converted into law, with amendments, by Law No 56 of 29 April 2024 broadened COLAF’s remit in line with needs linked to implementation of the NRRP. Specifically:</p> <ul style="list-style-type: none"> <li>- paragraph 1 extended COLAF’s functions under Article 3(1) of Presidential Decree No 91 of 14 May 2007 to combat fraud against the European Union within the meaning of Article 54(1) of Law No 234 of 24 December 2012 so that they now cover the NRRP too, the aim being to strengthen the overarching strategy of activities to prevent and combat fraud and other offences affecting NRRP funding, the cohesion policy for the 2021-2027 programming period and national funds linked with those funds in any way;</li> <li>- in accordance with paragraph 2, and without prejudice to Articles 6 and 7 of Decree-Law No 77/2021 converted into law, with amendments, by Law No 108/2021, for the</li> </ul>

---

**Member  
State****Response**

---

aforementioned functions COLAF is required, in particular, to:

request information on the steps taken by institutions, agencies and bodies to prevent and combat the fraud and other offences referred to in paragraph 1;

- encourage the signing of memorandums of understanding within the meaning of Article 7(8) of the aforementioned Decree-Law No 77/2021 and monitor their implementation;
- assess the appropriateness, including on the basis of the activity referred to in the first point of drafting proposals, including legislative proposals, to be submitted to the competent administrations or the steering committee referred to in Article 2 of the aforementioned Decree-Law No 77/2021.
- develop analysis activities, including in light of the trend in the results of action to prevent and combat fraud and other offences. For these purposes, paragraph 3 of the aforementioned Decree-Law extended COLAF's membership following the assignment of the new tasks under the provision in question.

More specifically, pursuant to Article 3(2) of Presidential Decree No 91/2007, the Committee is composed of:

- the Head of the Department for European Affairs at the Prime Minister's Office;
- the Commander of the Guardia di Finanza Unit for Combatting Fraud against the European Union, as mentioned in the next section;
- the directors-general of the offices of the Department for European Affairs;
- the directors-generals designated by the administrations involved in the fight against tax and agricultural fraud and in the correct use of EU funds, who are nominated by the Minister for European Affairs, Southern Italy, Cohesion Policy and the NRRP;
- members designated by the Joint Conference referred to in Article 8 of Legislative Decree No 281 of 28 August 1997.

Pursuant to Article 3(3) of Decree-Law No 19/2024, and in order to achieve the aims laid down in paragraphs 1 and 2 of that article, COLAF's membership has been supplemented with:

- as 'ex officio members', the coordinator of the NRRP Unit referred to in Article 2 of Decree-Law No 13/2023 converted into law, with amendments, by Law No 41/2023, the Head of the Department for Cohesion Policy and Southern Italy at the Prime Minister's Office, the coordinator of the Special Economic Zones (SEZ) Unit referred to in Article 10(2) of Decree-Law No 124/2023 converted into law, with amendments, by Law No 162/2023, the Chair of the Network of NRRP Anti-Fraud Contact Persons established at the State General Accounting Department at the Ministry of Economic Affairs and Finance and the Chair of the Coordination Committee established at the Ministry of the Interior pursuant to Article 39(9) of the Public Procurement Code laid down in Legislative Decree No 36 of 31 March 2023;
- as 'designated members', one representative each of the General Headquarters of the Carabinieri, the General Headquarters of the Guardia di Finanza, the Guardia di Finanza's Special Unit for Public Expenditure and Combatting Fraud against the European Union, the Italian Court of Auditors, the National Anti-Corruption Authority, the Financial Intelligence Unit at the Bank of Italy, the National Anti-Mafia and Anti-Terrorism Directorate, and the Central Criminal Police Directorate and Anti-Mafia Investigation Directorate at the Ministry of the Interior.

The performance of the tasks assigned to COLAF is facilitated by the presence, within the Department for European Affairs at the Prime Minister's Office, of the Guardia di Finanza Unit for Combatting Fraud against the European Union, established by the Prime Ministerial Decree of 11 January 1995, as COLAF's Technical Secretariat. The functions of that unit were laid down by Article 3(2) and (4) of Presidential Decree No 91/2007 and Article 54(2) of Law No 234 of 24 December 2012 and recently updated and better defined by Article 10 of the Decree of the Minister for European Affairs, Southern Italy, Cohesion Policy and the NRRP of 23 November 2023.

---

Member State	Response
	<p>More specifically, in accordance with the latter provision, the Guardia di Finanza Unit that acts as technical secretariat for COLAF:</p> <ul style="list-style-type: none"> <li>- reports to the Head of Department, performs advisory and guidance functions to coordinate the activities to fight against fraud and irregularities concerning, in particular, tax and the CAP and structural funds, and carries out the associated activities to share information with the European Commission;</li> <li>- in the areas within its remit, follows the work of EU bodies, in particular the Advisory Committee for the Coordination of Fraud Prevention (COCOLAF) and the Working Party on Combating Fraud (GAF), and oversees the adoption of the national position to be taken in those forums;</li> <li>- helps COLAF to perform all the tasks assigned to it, to implement the decisions taken during its deliberations and to carry out the initiatives decided upon;</li> <li>- in relation to COLAF's designation as the 'Anti-fraud coordination service' pursuant to Article 12a of Regulation (EU, Euratom) No 883/2013, it is responsible for facilitating cooperation and information exchange with OLAF, including of an operational nature, and for drawing up the national anti-fraud strategy;</li> <li>- manages the flow of communications concerning irregularity and fraud cases affecting European funds via the Irregularity Management System (IMS), ensuring interconnection with OLAF, the competent national central authorities and the managing authorities, including so as to resolve any technical problems that arise and ensure harmonised procedures;</li> <li>- analyses the data from the IMS, including for the purposes of general fraud risk assessment at national level and to make a comparison with how the fight against irregularity and fraud is developing at European level;</li> <li>- gathers information and data from the national administrations involved in fighting fraud against the EU and then answering the 'Questionnaires' to be sent to the European Commission on the basis of Article 325 TFEU, following the Commission's Recommendations and the guidance from other EU institutions on protecting the financial interests of the Union; in partnership with other national and foreign institutions, and also as part of projects financed by the EU, participates in training and study initiatives aimed at improving the fight against fraud, and ensures that correct information is provided on the actions taken by the EU and national institutions to protect the financial interests of the Union.</li> </ul>

Q.3.3 If “YES, we set up an anti-fraud governance structure” or “YES, we modified the existing anti-fraud governance structure” to Q.3.1, Which authorities have you newly included in your anti-fraud governance structures in 2024?

Response	Frequency	Percentage	Member States
EU fund managing authority	3	11.1%	CY, LV, IT
Other (please specify)	3	11.1%	LU, NL, ES
Judicial authority	2	7.4%	ES, IT
Dedicated agency fighting against conflict of interest	1	3.7%	IT
Dedicated agency fighting against organized crime	1	3.7%	IT
Dedicated anti-corruption agency	1	3.7%	IT

Response	Frequency	Percentage	Member States
Law enforcement authority	1	3.7%	IT
National audit authority	1	3.7%	IT
Public procurement authority	1	3.7%	IT
Tax administration authority	1	3.7%	IT

Following Q.3.3, please specify "Other".

Member State	Response
LU	Anti-fraud officer
NL	AFCOS is part off Customs and already responsible for revenue. New responsible will be the coordination of antifraud for expenditure
ES	Independent Authorities for the Protection of Whistleblower

Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure facilitates knowledge exchange and good practices to fight fraud.

Response	Frequency	Percentage	Member States
Effective	17	63.0%	IE, LU, HR, SE, EL, BE, AT, FI, LT, SI, CZ, ES, SK, DE, BG, PT, DK
Highly effective	7	25.9%	FR, HU, PL, MT, RO, LV, IT
Mildly effective	3	11.1%	NL, CY, EE

Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure is the ideal forum to elaborate a comprehensive risk assessment to support anti-fraud effort

Response	Frequency	Percentage	Member States
Effective	13	48.1%	LU, EL, BE, AT, LT, SI, HU, SK, DE, BG, PT, LV, DK

Response	Frequency	Percentage	Member States
Mildly effective	6	22.2%	HR, SE, NL, CZ, ES, CY
Highly effective	5	18.5%	FR, PL, MT, RO, IT
Neutral	3	11.1%	IE, FI, EE

Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure provides a comprehensive understanding of anti-fraud issues.

Response	Frequency	Percentage	Member States
Effective	16	59.3%	IE, LU, BE, AT, LT, CZ, HU, SK, DE, BG, MT, CY, EE, PT, LV, DK
Highly effective	6	22.2%	FR, EL, SI, PL, RO, IT
Mildly effective	4	14.8%	HR, SE, NL, ES
Neutral	1	3.7%	FI

Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure contributes to the development / update of anti-fraud policies/strategies at the national level.

Response	Frequency	Percentage	Member States
Effective	15	55.6%	LU, EL, BE, AT, FI, LT, SI, ES, HU, SK, PL, DE, BG, CY, DK
Highly effective	5	18.5%	FR, MT, RO, LV, IT
Mildly effective	3	11.1%	HR, CZ, PT
Neutral	3	11.1%	IE, NL, EE
Not applicable	1	3.7%	SE

Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure responds quickly to new threats in the anti-fraud environment.

Response	Frequency	Percentage	Member States
Effective	18	66.7%	IE, LU, EL, BE, AT, FI, LT, SI, CZ, ES, HU, DE, BG, MT, EE, RO, LV, DK
Highly effective	3	11.1%	FR, PL, IT
Mildly effective	3	11.1%	HR, SK, PT
Neutral	3	11.1%	SE, NL, CY

Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure contributes to drafting anti-fraud legislation.

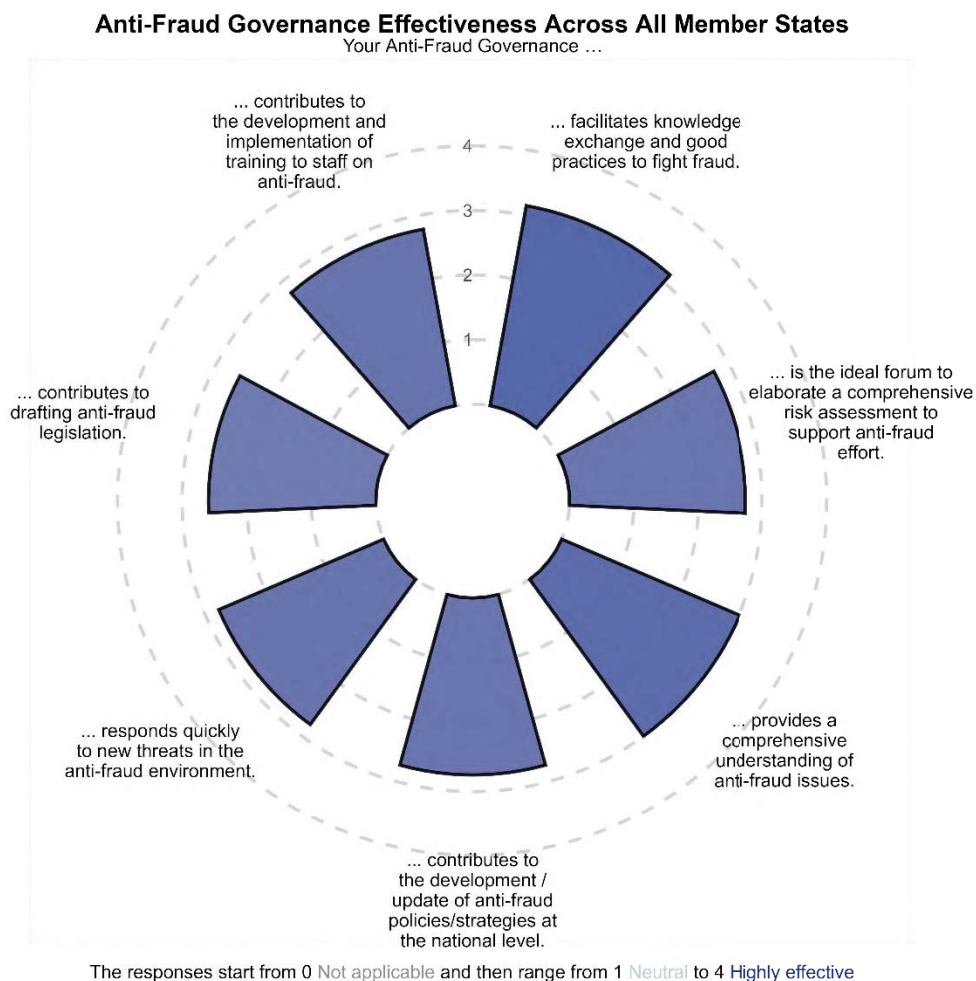
Response	Frequency	Percentage	Member States
Effective	13	48.1%	EL, FI, LT, SI, CZ, ES, HU, SK, PL, DE, BG, CY, PT
Highly effective	5	18.5%	FR, MT, RO, LV, IT
Mildly effective	4	14.8%	HR, SE, NL, EE
Neutral	3	11.1%	IE, LU, BE
Not applicable	2	7.4%	AT, DK

Q.3.4 Please rate the effectiveness of the statements below.: Your anti-fraud governance structure contributes to the development and implementation of training to staff on anti-fraud.

Response	Frequency	Percentage	Member States
Effective	10	37.0%	EL, BE, FI, LT, SI, CZ, SK, DE, CY, EE
Highly effective	9	33.3%	FR, ES, HU, PL, MT, RO, PT, LV, IT
Mildly effective	3	11.1%	HR, SE, NL

<b>Response</b>	<b>Frequency</b>	<b>Percentage</b>	<b>Member States</b>
Neutral	3	11.1%	IE, LU, BG
Not applicable	2	7.4%	AT, DK

## Polarplot of the Average Level of Self-Reported Governance Effectiveness in Anti-Fraud Efforts Across All Member States



**Q.3.5** Could you describe any best practices or innovative methods that your anti-fraud governance structures have implemented to enhance effectiveness and collaboration?

Member State	Response
IE	n/a
LU	Not applicable.
HR	<p>Contribution from Agency for the Audit of European Union Programmes Implementation System (ARPA):</p> <p>It was the development of National irregularity management guidelines with all relevant annexes and appendices. The MCS structures need such document as a kind of “cookbook” with descriptions, processes, steps, etc.</p> <p>Contribution from Ministry of Finance, Customs Administration:</p> <p>Greater use of customs mutual administrative assistance framework (for example strengthening of</p>



Member State	Response
	cooperation with neighbouring third countries).
	<p>Contribution from Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development:</p> <p>From the point of view of the managing authority (Ministry of Agriculture, Forestry and Fisheries), we can say that we are constantly working to improve the exchange of information with the Paying agency, which is the implementing body in the system of management and controls of EU agricultural funds.</p>
SE	<p>Cooperation between the SEFI Council and the various working groups under the SEFI Council enhances collaboration and knowledge sharing in anti-fraud work. A vibrant dialogue within the organisation but also with other organisations to raise awareness of the issues. Cooperation and exchange of information and knowledge between authorities. Exchange of staff between authorities. Targeted tailor-made training requested by individual authorities is provided through the SEFI Council and the Swedish Economic Crime Authority upon request.</p>
NL	<p>NAFS is being prepared (concept). Organising network meetings with management authorities and different other parties involved with the expenditure like national audit agency in order to establish a better cooperation.</p>
FR	<p>At national level, the MICAF, in partnership with the lead managing directorates, oversees attentively 10 national anti-fraud operating groups (Groupes opérationnels nationaux anti-fraude - GONAF). The task of these GONAF is to break down barriers by sharing information and analysis, mapping risks jointly, and developing action strategies and coordinated investigations. This includes, inter alia, identifying and combating complex, organised fraud more effectively by promoting better coordination of administrative and judicial action.</p>
EL	<p>Recovery and Resilience Facility Coordination Agency (RRFA): The anti-fraud cooperation network for projects which are implemented using funding from the Recovery and Resilience Fund, which is made up of the competent ministries, large implementing bodies for NRRP actions/projects and the NRRP Coordination Service. The Greek Anti-Fraud Coordination Service (NTA/AFCOS) and the Control Authority of the Recovery and Resilience Facility may participate in the network. The Independent Anti-Fraud Coordination Service of the National Transparency Authority (NTA) has organised an online communication platform between competent national bodies where accredited users can exchange information, be informed and participate in discussion forums to resolve issues.</p>
BE	<p>ERDF, JTF and RRF at the SPW: For the SPW, a robust anti-fraud culture, a regularly updated management and control system, the establishment of procedures, the transposition of the Whistleblowing Directive through the appointment of contact persons for integrity in 2024, and the drafting of a full training programme that is to be implemented in 2025.</p>
AT	<p>No information.</p>
FI	<p>At the request of the administrative authority, the intermediate bodies for the EU's regional and structural policy programme have nominated their contact persons for fraud prevention. The persons in question constitute a network which is used for the sharing of up-to-date information and the dissemination of good practices. Similar practices are also employed in other EU programmes.</p>

Member State	Response
LT	-
SI	<p>The Ministry of Cohesion and Regional Development (MKRR), in its role as MA for the implementation of the European cohesion policy programme, has concluded an agreement with the Agency of the Republic of Slovenia for agricultural markets and rural development [ARSKTRP] – the manager of the European Agricultural Fund – on cooperation between the two bodies in order to prevent double funding from public sources. The two bodies agreed/committed to exchange data about beneficiaries, public invitations to tender, etc. with a view to preventing double funding from the two different EU funds, to keep each other informed of any matches and to carry out an additional review where there is a risk of double funding</p>
CZ	<p>Start of work on using ARACHNE data for analytical activities. The Directorate-General for Finance understands that the data contained in IS ReD are a valuable source of information that will allow the identification of key trends, patterns, and risk profiles in conjunction with ARACHNE. These analyses serve as an important tool for planning, allocation of funds and control activities of other government bodies. The Working Group on the Publication of Subsidy Data, which includes representatives from the Ministry of Finance and the Directorate-General for Finance, was launched in April 2024. The Working Group is to define the requirements for the integration of archived data from ReD and to coordinate the activities of the IISSP (integrated State treasury information system) process teams related to the preparation and subsequent implementation of the publication of subsidy data in the Monitor, i.e. to ensure coordination of the data collection activities necessary for the publication of the subsidy data and the activities of the Ministry of Finance and the Financial Administration related to the provision of the data necessary to ensure the Directorate-General for Finance's own internal processes (e.g. ensuring analytical search and control processes for subsidies). Work has started on amending the legislation, in particular amendments to Act No 218/2000 on budgetary rules. At the same time, we have automated the transfer of State budget subsidy and grant data from the RISPF (computerised information system for programme financing) to the Management Information System, which is part of the IISSP and where the requirements for publishing such data on the open-access Monitor website (Monitor – Information Portal of the Ministry of Finance) are now being defined.</p> <p>Improving synergies with law enforcement and judicial authorities. Improving the satellite monitoring system for agricultural land.</p> <p>A proven approach is to provide staff with training on preventing corruption and fraud as soon as they take up their duties, introducing codes of ethics, and introducing checklists and the four-eyes control principle for all operations and payments. It is essential to apply precaution and continuous awareness of the risk of fraud at all stages in the implementation of the National Recovery Plan. Project risk cards have been introduced as part of the internal sharing.</p>
ES	<p>Coordination meetings have been held with the units, as well as working groups and training courses. In addition, new manuals and protocols have been produced and disseminated.</p>
HU	<p>Cooperation between organisations involved in the fight against fraud is ensured both formally and through cooperation agreements with detailed arrangements. In addition, the Hungarian AFCOS organises a number of professional events per year to which anti-fraud actors are invited to present and disseminate a priority theme, and where workshops permit both exchanges of experience and peer-to-peer reflection.</p>

Member State	Response
SK	<p>At the level of MA 2021-2027, the following measures were implemented in the recent past, which are also related to the issue of combating fraud. Internal control aimed at compliance with the duties of the employees of the Programme Slovakia Managing authority in connection with the conflict of interests. Establishment of working groups for fraud risk management for the Programme Slovakia, the Interreg Slovakia – Czech Republic and Interreg Slovakia – Austria Programs and the Recovery and Resilience Plan of the Slovak Republic (component 17). Adoption of the "Anti-Fraud Policy" of</p> <p style="text-align: center;">MIRRI</p> <p style="text-align: right;">SR.</p> <p>Authorities involved in the implementation of EU funds use a unified IT monitoring system, which contains detailed information about the given cases. Regular communication and exchange of information among all authorities (CA/PA, IB, AA, law enforcement authorities, etc.) Issue/update manuals and guidelines on the protection of the EU's financial interests. Train the employees, strengthen and streamline cooperation among AFCOS partners in identifying new methods of harming the EU's financial interests. Provide the public conditions for reporting potential fraud, which also helps to protect the EU's financial interests. Slovak RRF: PIF related training activities for employees of implementing bodies (line ministries) and NICA (National Implementation and Coordination Authority); round tables organised by NICA to discuss specific issues with the line ministries.</p>
PL	<p>The Institution Coordinating the Partnership Agreement organises annual conferences on the topic of checks and irregularities in the spending of structural funds and co-financing under the Cohesion Fund, which are attended by representatives of the institutions involved in the implementation of the Structural Funds and the Cohesion Fund, including national and regional managing authorities and selected intermediate bodies and audit authorities. The topic of each conference depends on the current themes that are important from the point of view of control and prevention of irregularities. In different years, representatives of the European Commission, the National Public Prosecutor's Office or the Police also participated in those meetings.</p> <p>The Institution Coordinating the Partnership Agreement has developed and made available information and guidance materials on conflicts of interest in the form of YouTube podcasts. The materials are mainly aimed at the staff of the institutions that manage and control the spending of EU funds. The materials discuss key issues relating to conflicts of interest, including how to tackle conflicts of interest at the different stages of programme and project implementation.</p> <p>Regular anti-fraud training for staff is provided at the Paying Agency. A list of signs of fraud has been drawn up and it is kept up to date. Work is underway to adapt (extend) internal applications by adding new tools (e.g. Register of artificial conditions) that may be useful in the fight against fraud.</p>
DE	<p>The Bremen ERDF Managing Authority:</p> <ul style="list-style-type: none"> <li>• Regular four fixed meetings between the managing authority and intermediate bodies.</li> <li>• Staff awareness training.</li> </ul>
BG	<p>With the professional support and expertise of Department 08 within PORB, as a specialized unit in the structure of the Prosecutor's Office in Bulgaria, four seminars for prosecutors, investigators, reporting and executive authorities and representatives of the EPPO office in Sofia, Bulgaria were organized and conducted. These specialized events were organized and funded by the America for Bulgaria Foundation as a part of a three-year "Supporting the Counteraction to Fraud and Organized Crime" project.</p> <p>Following the initiative of the Head of the 08 Department series of events and work meetings with representatives of the reporting and responsible institutions and authorities aiming better</p>

Member State	Response
	<p>cooperation and understanding of the specific requirements of matters in the work of the judicial system were held throughout 2024.</p> <p>Prosecutors from the 08 Department actively take part in all international events and forums in the 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.</p> <p>Again, as an initiative of the 08 Department cooperation agreement on interaction and cooperation between the Prosecutor's Office of the Republic of Bulgaria and the Ministry of Interior in countering offenses affecting the financial interests of the European Union was signed on 11.06.2024.</p>
MT	The implementation of a Central Document Repository System (CDRS), in line with Action Points 13 and 14 of the Maltese NAFCS, as well as Malta's RRP commitments.
CY	N/A
EE	<p>Our network collaborates as needed, we have at least annual regular meeting, and we organize specific training courses to support and share our skills.</p> <p>We have proposed to our national investigative bodies to analyse all grants data. This cooperation could contribute to the identification of the potential threats, vulnerabilities and fraud. Complex fraud cases cannot be detected through administrative-level controls only.</p>
RO	Operationalisation of professional anti-fraud networks, in permanent communication with each other, in the following areas: policies and legislation, vocational training, communication, investigations, risk analysis, reporting of irregularities, debt recovery, contributions to the EU budget and European cooperation.
PT	Conclusion of protocols between the Funds' coordinating bodies and the judicial authorities
LV	In 2024 we implemented "job shadowing" initiative, where employees of anti-fraud governance structures could "shadow" jobs of employees from other institutions. For example, employees of the law enforcement authorities could participate in the project on-the-spot checks carried out by the EU managing authority, gaining better understanding about project implementation and administration.
DK	<p>The members of the Danish AFCOS meet at least once a year to discuss changes to existing practices, to share best practices and to facilitate a common understanding of the task.</p> <p>The members of the Danish AFCOS meet with representative from the European Court of Auditors at a yearly meeting facilitated by the Danish AFCOS. The Court of Auditors presents their annual report concerning the previous financial year. The members of the Danish AFCOS get to ask questions and gain a better understanding of contemporary topics.</p> <p>The Danish AFCOS regularly shares news, information and upcoming events with member of the AFCOS.</p>
IT	With regard to the strengthening of anti-fraud governance, the Italian AFCOS ensures ongoing, systematic interconnection between all the authorities and administrations responsible in various capacities for fighting and preventing fraud, including through targeted consultations aimed at

Member State	Response
	<p>determining the national position to be taken at interinstitutional and EU level and at disseminating new guidelines and lines of action for the fight against fraud, risk analysis and improving the procedures for protecting the EU budget, including in relation to the NRRP.</p> <p>With input from all institutions making up the AFCOS, two documents have been drafted concerning:</p> <ul style="list-style-type: none"> <li>a. ‘Measures to prevent and combat fraud and other offences against the NRRP’, which contains a full survey of all the measures in place to prevent and combat such fraud, including measures introduced specifically for the NRRP and also general measures under national law that are directly effective as preventive safeguards in relation to the NRRP too;</li> <li>b. the ‘Main risk indicators for NRRP fraud’, which gives a full overview of the ‘anomaly indicators’ developed by various EU and national institutions to guide the control actions for situations that need to be investigated.</li> </ul> <p>A new National Anti-Fraud Strategy (NAFS) has been prepared taking on board guidelines and proposals from all the institutions involved in protecting the financial interests of the EU. This is part of a broad process agreed upon collegially by the Committee that has also led to the production of an Action Plan for 2024-2027. There will be monitoring of the correct implementation of the profiles within the remit of the various administrations, and of the guidance and targets in the aforementioned Action Plan, which gives a forward-looking view of the objectives that the various national authorities envisage achieving in the 2024-2027 reference period, specifying the indicators and timescales for each of the four stages of the ‘anti-fraud cycle’: prevention, detection, investigation, recovery and penalties.</p> <p>Lastly, with regard to the new functions linked to implementation of the NRRP, and pursuant to Article 3 of Decree-Law No 19 of 2 March 2024, the AFCOS closely follows the steps taken by institutions, agencies and bodies to prevent and combat fraud and other offences in the specific sector of the cohesion policy and national funds linked with it in any way, monitors the memorandums of understanding signed with the Guardia di Finanza by the central administrations responsible for NRRP measures, the regions, the autonomous provinces of Trento and Bolzano, local authorities and other public entities, assesses any proposals, including legislative proposals, to be submitted to the competent administrations or the NRRP Steering Committee at the Prime Minister’s Office and develops analysis activities, including in light of the trend in the results of action to prevent and combat fraud and other offences.</p> <p>Particular attention is also given to communication and training. In this connection, two projects have been developed and are co-financed by the European Commission as part of the Union Anti- Fraud Programme:</p> <ul style="list-style-type: none"> <li>1) in cooperation with Luiss University in Rome, a European project called ‘Better Knowledge for Next Generations’ (BETKONEXT).</li> </ul> <p>This project involves a comparative law study and targeted training activities aimed at improving cooperation and coordination between academia and the Member States’ AFCOSs so as to achieve ever higher standards in the protection of the financial interests of the European Union. The project therefore has the specific objective of conducting a scientific research project aimed, in particular, at assessing the fitness for purpose of the existing regulatory tools and at perfecting multilateral and multi-level cooperation between institutions, academia and control bodies.</p> <p>Intense international cooperation will see the involvement of national institutions (including the National Anti-Corruption Authority, the Guardia di Finanza, the Financial Intelligence Unit at the Bank of Italy and the Central Criminal Police Directorate), EU institutions (OLAF, EPPO and</p>

Member State	Response
	<p>Europol), experts from universities and AFCOSs in the EU countries involved in the project (Belgium, Poland and Spain) and Italian and foreign students;</p> <p>2) in cooperation with Sapienza University of Rome, another European project called 'Fraud Repression through Education' (FRED 2). Through intense cooperation between Italian and European universities and the AFCOSs of the participating foreign countries (Belgium, Finland and Greece), the project objectives are to:</p> <ul style="list-style-type: none"> <li>- develop an experiential co-lab-learning course with the participation of academics and professionals so as to develop innovative, value-for-money approaches that will provide participants with better know-how for determining fraud risks and comparing control strategies in the fight against irregularities and fraud against the EU budget;</li> <li>- create a European task force of academics and professionals that will develop a pilot study for analysing risk profiles for possible illegal behaviours or situations of improper use of EU funds;</li> <li>- set up, in parallel, a permanent Anti-Fraud Observatory, intended to have a trans-national European dimension in future, that will allow the new network to endure through relationships aimed at improving awareness of fraud and other illegal activities by strengthening trans-national and multidisciplinary cooperation.</li> </ul> <p>Lastly, in the area of training, it is important to stress the objective, set in the NAFS Action Plan, of ensuring that the culture of combatting fraud against EU funds is also spread to national bodies responsible for checks in other sectors.</p> <p>In particular, a training activity was run for inspection staff of the National Labour Inspectorate (INL) with the aim of providing them with the necessary competencies to identify, analyse and assess the various types of irregularity/fraud affecting the agricultural policy, cohesion policy and NRRP and to identify the types of penalties that apply and the associated reports to be sent to the competent bodies.</p>

#### Q.3.6 Has there been any change regarding the staffing of your national anti-fraud structure coordinating the anti-fraud governance (AFCOS) in 2024?

Response	Frequency	Percentage	Member States
No change in staffing levels	12	44.4%	SE, FI, LT, SI, CZ, ES, SK, DE, BG, EE, LV, DK
Cannot assess / Not applicable	4	14.8%	IE, FR, AT, CY
Other (please specify)	4	14.8%	NL, BE, PL, MT
Same staffing levels, but more efficient	4	14.8%	LU, HU, RO, IT
Increased staffing with the necessary expertise	2	7.4%	HR, PT
Staffing levels decreased	1	3.7%	EL

Following Q.3.6, please specify "Other".

Member State	Response
NL	Setting up coordination antifraud for expenditure as part of AFCOS
BE	AFCOS
PL	Due to the number of institutions cooperating in the area of fight against fraud, it is not possible to provide reliable information on the changes in staffing levels at each of these institutions.
MT	Three new employees joined the Maltese AFCOS in 2024, who are currently gaining the necessary expertise.

Q.3.7 What are the main challenges currently faced in enhancing the anti-fraud governance in your Member State?

Response	Frequency	Percentage	Member States
Greater cooperation needed among existing entities	21	77.8%	LU, HR, SE, NL, FR, EL, LT, SI, CZ, ES, SK, PL, DE, BG, CY, EE, RO, PT, LV, DK, IT
Need more expertise and skilled staff	13	48.1%	LU, HR, SE, FI, SI, ES, HU, SK, DE, BG, RO, PT, LV
More funding required	12	44.4%	LU, HR, FI, SI, CZ, ES, SK, DE, BG, EE, RO, LV
Legal or regulatory obstacles	7	25.9%	HR, SE, NL, ES, DE, BG, RO
Other (please specify)	5	18.5%	IE, BE, AT, MT, IT

Following Q.3.7, please specify "Other".

Member State	Response
IE	There is no national anti-fraud strategy in place -- not a challenge just a statement.
BE	AFCOS



Member State	Response
AT	No information.
MT	No main challenges are currently being faced.
IT	<p>It would be appropriate for the national AFCOSs to be fully and effectively involved in the implementation of OLAF's recommendations. The Guardia di Finanza Unit at the Prime Minister's Office, as Technical Secretariat of COLAF, has asked OLAF for this on several occasions, and it was specifically envisaged in the European Commission's letter ref. ARES (2013)3403880 of 4 November 2013 providing guidance on the main tasks and responsibilities of an AFCOS.</p> <p>More specifically, as envisaged in the aforementioned 2013 ARES letter, when OLAF recommendations are being implemented, the AFCOS should facilitate the exchange of information between the national authorities involved, ensure the effective exchange of relevant information with OLAF, particularly as regards recovery of EU funds used improperly, and report to OLAF on the actions taken following the information sent pursuant to Article 11, paragraphs 1 et seq., of Regulation (EU, Euratom) No 883/2013.</p>

Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6): Increased funding / financial assistance

Response	Frequency	Percentage	Member States
5	8	29.6%	HR, NL, FR, AT, SI, DE, CY, EE
6	6	22.2%	LU, BE, CZ, BG, RO, IT
3	5	18.5%	IE, LT, HU, MT, PT
4	4	14.8%	ES, SK, PL, LV
Support not needed	3	11.1%	SE, EL, DK
2	1	3.7%	FI

Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6): Training programs for staff

Response	Frequency	Percentage	Member States
6	13	48.1%	FR, BE, AT, FI, SI, ES, SK, DE,



Response	Frequency	Percentage	Member States
			BG, RO, PT, DK, IT
4	5	18.5%	CZ, HU, MT, CY, EE
5	5	18.5%	SE, NL, EL, LT, HR
3	4	14.8%	IE, LU, PL, LV

Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6): Facilitated cooperation initiative / sharing good practices among Member States

Response	Frequency	Percentage	Member States
6	10	37.0%	FR, EL, BE, SI, HU, BG, RO, PT, DK, IT
4	8	29.6%	LU, HR, SE, NL, AT, ES, SK, DE
5	5	18.5%	LT, PL, MT, CY, EE
3	3	11.1%	IE, FI, CZ
1	1	3.7%	LV

Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6): Guidance on legal or regulatory framework adjustments

Response	Frequency	Percentage	Member States
4	7	25.9%	LU, NL, PL, BG, CY, IT, HR
5	6	22.2%	EL, FI, SK, DE, PT, LV
6	6	22.2%	SE, BE, AT, ES, RO, DK

Response	Frequency	Percentage	Member States
3	5	18.5%	IE, FR, LT, SI, HU
2	3	11.1%	CZ, MT, EE

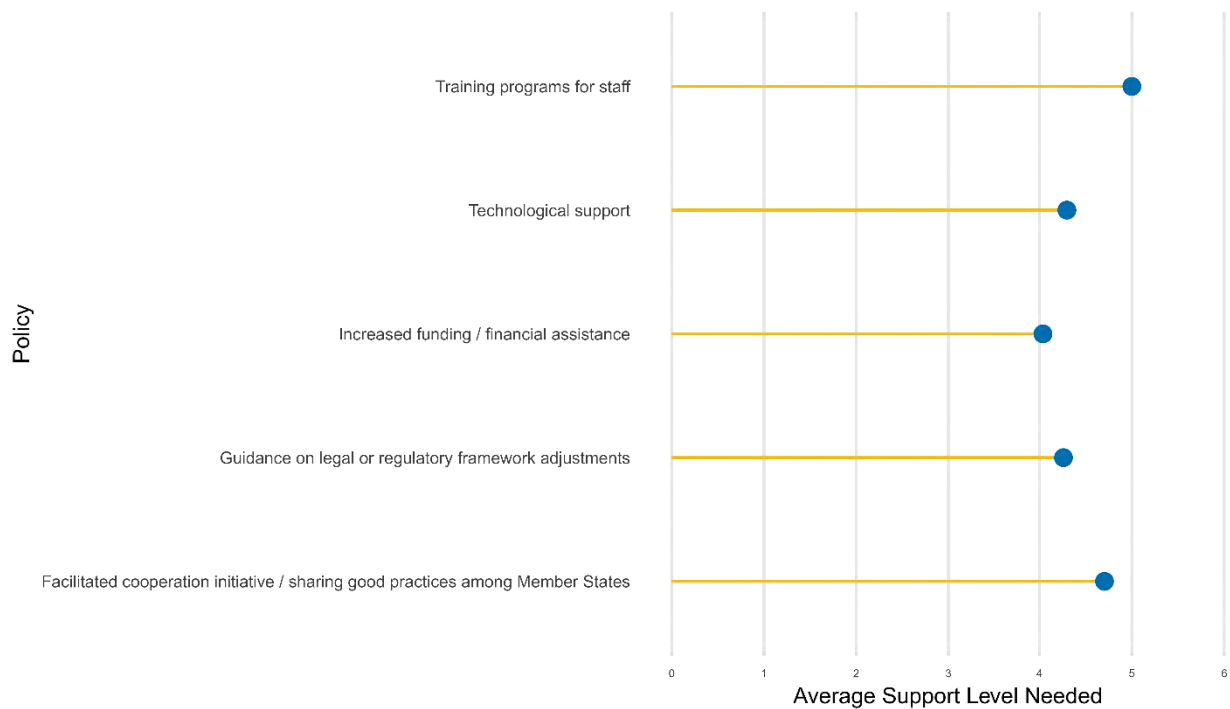
Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6).: Technological support

Response	Frequency	Percentage	Member States
5	7	25.9%	NL, EL, SI, CZ, SK, DE, BG
6	7	25.9%	FR, BE, AT, ES, CY, RO, IT
3	5	18.5%	IE, LU, SE, HU, MT
4	5	18.5%	FI, LT, EE, PT, HR
2	2	7.4%	PL, LV
Support not needed	1	3.7%	DK

Q.3.8 What type of support from the EU would you need to address the challenges identified in improving your anti-fraud governance? Please rank the following proposition from least important (1) to the most important (6).: Other (please specify in the following question)

Response	Frequency	Percentage	Member States
Support not needed	21	77.8%	LU, HR, NL, FR, AT, FI, LT, SI, CZ, ES, HU, SK, PL, DE, BG, MT, CY, RO, PT, LV, DK
6	3	11.1%	EL, BE, IT
2	1	3.7%	SE
3	1	3.7%	IE
5	1	3.7%	EE

**Bar plot of the Average Level of Support Requested for Anti-Fraud-Policy Across All Member States**  
**Average Level of Support Requested for Anti-Fraud Policy Across All Member States**



Q.3.9 If you selected “Other” to Q.3.8, please specify any other types of support you would need and its importance

Member State	Response
IE	hard to answer a Likert scale across a number of MA's
SE	It would be good to receive information and intelligence earlier, if the Commission detects, e.g., problems or suspected crimes in any area – rapid sharing
EL	The answers and detail given above cover the response to this question.
BE	ERDF, JTF and RRF at the SPW: Fraud is often international, while the European regulatory framework and the national or regional regulatory frameworks very often hinder access to the data required for the fight against fraud. A specific example is the collection and analysis of data on the beneficial owners of fund beneficiaries and their contractors. This data is easily available at national level but extremely difficult to obtain from outside the country. The European regulatory framework should allow direct access to this data whenever it is required by sector-specific regulations. The EU should collate the national data of its Member State and make this data available to the managing authorities rather than requiring them to have theoretical access via individual procedures that differ between the Member States. Such data could be integrated into ARACHNE, for example.
EE	Proper pan-European databases that can analyse data and identifying risks. The same rules for all funds and simplification of rules.
IT	As envisaged in the aforementioned 2013 ARES letter, when OLAF recommendations are being implemented, the AFCOS should facilitate the exchange of information between the national authorities involved, ensure the effective exchange of relevant information with OLAF, particularly

Member State	Response
	as regards recovery of EU funds used improperly, and report to OLAF on the actions taken following the information sent pursuant to Article 11(6) of Regulation (EU, Euratom) No 883/2013.

Q.3.10 Please feel free to share any additional thoughts or experiences you have regarding the topics discussed in this section.

Member State	Response
IE	n/a
LU	Not applicable.
HR	-
SE	The EU currently offers financial support for developing, e.g., anti-fraud tools: The dilemma is that the administrative burden of applying for and receiving such aid is so heavy that it greatly discourages Swedish authorities from applying for such aid.
NL	N/A
FR	x
EL	There must be cooperation at both national and European level between all the competent authorities involved in order to effectively address fraud linked to EU funding. This is the basis for the development of any successful national strategy which, in combination with the ultimate integration of new technologies in all aspects of public administration, can play a very important role in meeting the new challenges of our digital era.
BE	/
AT	No information.
FI	Administrative arrangements for fraud prevention in the Member States are a competence of the Member States.
LT	-
SI	more training, would be appreciated
CZ	-
ES	In a country as decentralised as Spain, coordination between all the entities that form part of the anti-fraud architecture is much more complicated.
HU	We consider the exchange of good practices in the Member States under question 3.8 as a priority, for which OLAF could provide an excellent platform with the help of the working groups under OLAF's authority. The effectiveness and efficiency of the fight against fraud in a context that increasingly focuses on digital solutions largely depends on Member States mobilising their

Member State	Response
	resources (such as expertise or IT solutions) individually and potentially in fragmentation or exploiting synergies in cooperation.
SK	X
PL	None
DE	-
BG	N/A
MT	In terms of Article 23 of the Internal Audit and Financial Investigations Act (Cap. 461 of the Laws of Malta), Malta has a Co-ordinating Committee 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'.
CY	N/A
EE	It is difficult to give nationwide answers to such detailed questions. Institutions have different tasks and develop at different paces; it means their answers are opposite. For the sake of comparability, please distinguish between topics (investigative-, implementing institutions etc.) in the next questionnaires.
RO	N/A
PT	Sharing best practices could help to improve the functioning of the existing governance structures.
LV	NA
DK	Nothing to report.

#### Q.4.1 Which national services were consulted to reply to this questionnaire?

Member State	Response
IE	all MA's
LU	Managing Authority / ESF
HR	Ministry of Agriculture, Forestry and Fisheries, Directorate for Support in Agriculture and Rural Development - Managing Authority for the Rural Development Programme 2014.-2022. and for the Strategic Plan of the Common Agricultural Policy 2023.-2027. Ministry of Labour, Pension System, Family and Social Policy, Directorate for the Management of EU Operational Programmes - Managing Authority for the Operational Programme Efficient Human Resources 2014-2020 and Programme Efficient Human Resources 2021-2027. Ministry of Regional Development and EU funds - Directorate for the Implementation of the Operational Programmes and Financial Instruments - Managing Authority for the Operational Programme Competitiveness and Cohesion 2014-2020 and Programme Competitiveness and

Member State	Response
	<p>Cohesion 2021-2027.</p> <p>Ministry of Finance, Customs Administration</p> <p>Ministry of Finance, Tax Administration</p> <p>Ministry of Agriculture, Forestry and Fisheries, Directorate of Fisheries - Managing Authority for Operational Programme for Maritime Affairs and Fisheries 2014-2020 and the Programme for fisheries and aquaculture 2021.-2027.</p> <p>Agency for the Audit of European Union Programmes Implementation System (ARPA) – The Audit Authority</p> <p>Croatian AFCOS Unit</p>
SE	Implementing authorities and Swedish AFCOS
NL	Departments of Finance, economic affairs, social affairs and agriculture, fisheries, food security and nature
FR	MICAF, CAP, cohesion funds
EL	<p>1. Ministry of Economy and Finance,</p> <ul style="list-style-type: none"> <li>- 1.1. Secretariat-General for Fiscal Policy Directorate-General for Audits of Co-financed Programmes Financial Audit Committee,</li> <li>- 1.2. Secretariat-General for Tax Policy and Public Property Directorate-General for the Financial and Economic Crime Unit,</li> <li>- 1.3. Secretariat-General for the Partnership Agreement for Regional Development,</li> <li>- 1.3.1. Special Service – Authority for Certification and Verification of Co-financed Programmes,</li> <li>- 1.3.2. ESPA National Coordination Authority Directorate-General for Institutional and Operational Support for the Partnership Agreement for Regional Development (ESPA) Special Service for Institutional Support and Information Systems (EYTHYPS),</li> <li>- 1.3.3. Special Service for State Aid and Financial Tools,</li> <li>- 1.4. Recovery and Resilience Facility Coordination Agency.</li> </ul> <p>2. Ministry of Citizen Protection Financial Police Directorate.</p> <p>3. Ministry of Justice.</p> <p>4. Ministry of Rural Development and Food,</p> <ul style="list-style-type: none"> <li>- 4.1. Office of the Secretary-General for Rural Policy and International Relations,</li> <li>- 4.2. Directorate-General for Administrative Services and e-Government Directorate for Legislative Initiative and Management of Infringements.</li> </ul> <p>5. Payment and Control Agency for Guidance and Guarantee Community Aid (OPEKEPE).</p> <p>6. Ministry of Migration and Asylum Special Service for the Coordination and Management of Migration and Home Affairs Programmes.</p> <p>7. National Transparency Agency.</p> <p>8 Independent Authority for Public Revenue,</p> <ul style="list-style-type: none"> <li>- 8.1. Office of the Governor,</li> <li>- 8.2. Directorate-General for Customs and Excise,</li> <li>- 8.3. Coordination Operational Centre for combating smuggling (SEK).</li> </ul> <p>9. Single Public Procurement Authority.</p>
BE	<p>Federal Public Economy Service - Coordination of Fraud Control – AFCOS BE</p> <p>Federal Public Finance Service</p>

Member State	Response
	<p>Federal Public Policy and Support Service</p> <p>Federal Public Justice Service</p> <p>Communities (German-speaking, Flemish &amp; French)</p> <p>Regions (Brussels - Capital, Flemish &amp; Walloon)</p> <p>European Social Fund Brussels-Capital</p> <p>European Social Fund Flanders</p> <p>European Regional Development Fund Brussels-Capital</p> <p>European Regional Development Fund, Recovery and Resilience Facility &amp; European Social Fund Wallonia (The SPW services involved in protecting EU interests in the fight against fraud)</p> <p>European Regional Development Fund Flanders</p> <p>Walloon Paying Agency</p> <p>Agency for Agriculture &amp; Fisheries</p> <p>Federal Police</p>
AT	<p>All federal ministries. Replies were received from the Federal Ministry of Agriculture, as well as the Federal Ministry of Labour and Economy (ESF Managing Authority and ESF Audit Authority).</p>
FI	<p>Ministry of Agriculture and Forestry</p> <p>Ministry of the Interior</p> <p>Ministry of Economic Affairs and Employment</p> <p>Ministry of Finance</p> <p>Police of Finland</p> <p>Finnish Food Authority</p> <p>Finnish Customs</p> <p>State Treasury</p> <p>Tax Administration</p>
LT	<p>Special Investigation Service of the Republic of Lithuania, Customs of the Republic of Lithuania, Ministry of the Interior of the Republic of Lithuania, Ministry of Finance of the Republic of Lithuania,</p> <p>Prosecutor General's Office, Ministry of Agriculture of the Republic of Lithuania, Public Procurement Office.</p>
SI	<p>Ministry for Cohesion and Regional development, FARS-Financial Administration of the Republic of Slovenia, Agency for Agricultural Markets and Rural Development (AAMRD), the Recovery and Resilience Office, Supreme State Prosecutor's Office of the Republic of Slovenia and others.</p>
CZ	<p>National Coordination Authority, Delivery Unit, Managing authorities, Component owners, Police of the Czech Republic - National Organized Crime Agency, Prosecutor General's Office, General Customs Directorate, General Financial Directorate</p>
ES	<p>European Social Fund Administration Unit (UAFSE)</p> <p>Sub-Directorate General Economic Management and European Funds (managing authority for AMIF)</p> <p>Sub-Directorate General Economic Sustainability and Social Affairs ( managing authority for</p>

Member State	Response
	<p>European Maritime, Fisheries and Aquaculture Fund)</p> <p>Sub-Directorate General Inspection and Control (Directorate-General for European Funds)</p> <p>Sub-Directorate General European Territorial Cooperation (managing authority for ETC programmes)</p> <p>Sub-Directorate General Agricultural Funds- FEAGA (Spanish Agricultural Guarantee Fund - coordinating body of the paying agencies)</p> <p>FEAGA Internal Audit Division</p> <p>Sub-Directorate General ERDF (managing authority for ERDF)</p> <p>Sub-Directorate General Planning and Management of Infrastructures and Resources for Security (managing authority for ISF))</p> <p>Sub-Directorate General for the Management of the National Recovery Plan ( Directorate General for the Recovery and Resilience Plan and Mechanism, General Secretariat for European Funds)</p> <p>State Agency for Tax Administration (AEAT)- Customs and Excise Department</p> <p>State Agency for Tax Administration (AEAT)- Department of Financial and Tax Inspection.</p> <p>Undersecretariat of the Ministry of Agriculture, Fisheries and Food -Anti-fraud and Internal Control Unit (Civil Guard)</p> <p>National Police</p>
HU	<p>The National Development Centre Internal Audit and Integrity Directorate, OLAF Coordination Office at the Central Management of the National Tax and Customs Administration (AFCOS).</p>
SK	<p>Bratislava Self-Governing Region - Interact, Ministry of Transport of the Slovak Republic, Ministry of Finance of the Slovak Republic, Ministry of Investments, Regional Development and Information of the Slovak Republic, Ministry of Agriculture and Rural Development of the Slovak Republic, Ministry of Health of the Slovak Republic, Ministry of the Environment of the Slovak Republic, Supreme Audit Office of the Slovak Republic, Antimonopoly Office of the Slovak Republic, Public procurement office, Government Office of the Slovak Republic, Ministry of Justice of the Slovak Republic, Ministry of Labour, Social affairs and family of the Slovak Republic, Ministry of Economy of the Slovak Republic, Ministry of the Interior of the Slovak Republic, Ministry of Culture of the Slovak Republic, Financial Directorate of the Slovak Republic, General Prosecutor's Office of the Slovak Republic and Ministry of Education, Research, Development and Youth of the Slovak Republic.</p>
PL	<p>Ministry of Finance (AFCOS)</p> <p>Ministry of Development Funds and Regional Policy (Partnership Agreement Coordinating Institution)</p> <p>The Agency for Restructuring and Modernisation of Agriculture (Paying Agency)</p>
DE	<p>The Federal ESF Managing Authority within the Federal Ministry of Labour and Social Affairs (BMAS)</p> <p>The Federal Ministry of Food and Agriculture (BMEL)</p> <p>The Saarland ESF Managing Authority</p> <p>Through the Federal Ministry of Economic Affairs and Climate Action (BMWK), the following managing authorities</p> <p>The Baden-Württemberg ERDF Managing Authority</p> <p>The Bremen ERDF Managing Authority</p> <p>The North Rhine-Westphalia ERDF Managing Authority</p>



Member State	Response
	<p>The Rhineland-Palatinate ERDF Managing Authority</p> <p>Investitions- und Förderbank Niedersachsen (Nbank), the intermediate body for the ERDF/ESF+ Managing Authority</p> <p>The Schleswig-Holstein ERDF Managing Authority</p> <p>The Thuringia ERDF Managing Authority</p>
BG	The Bulgarian AFCOS Council (Managing authorities, Audit authorities, Accounting Body, Customs Agency, National Revenue Agency, State Agency for National Security)
MT	To obtain the necessary replies, the Maltese AFCOS liaised with the Office of the Prime Minister - EU Funds, Equality, Reforms and Social Dialogue.
CY	AFCOS
EE	We sent the 2023 follow-up questionnaire to 12 institutions and received eight responses.
RO	<p>36 national services were consulted:</p> <p>The National Agency for Fiscal Administration, the Paying Agency for Rural Investments, the National Agency of Public Civil Servants, the Agency for Payments and Intervention for Agriculture, the Audit Authority, the Certification and Payment Authority, the Ministry of Internal Affairs, the Ministry of Agriculture and Rural Development, the Ministry of the Economy, Digitalisation, Entrepreneurship and Tourism, the Ministry of Culture, the Ministry of Development, Public Works and Administration, the Ministry of Education and Research, the Ministry of Energy, the Ministry of Labour, Family, Youth and Social Solidarity, the Ministry of Finance, the Ministry of Investments and European Projects,</p> <p>the Ministry of Justice, the Ministry of the Environment, Water and Forestry, the Ministry of Health, the Ministry of Transport and Infrastructure, the Secretariat-General of the Government, the North-East Regional Development Agency, the South-East Regional Development Agency, the South-Muntenia Regional Development Agency, the West Regional Development Agency - ADR West, the South-West Oltenia Regional Development Agency, the Bucharest Ilfov Regional Development Agency, the North-West Regional Development Agency, the Centre Regional Development Agency - ADR Centre.</p>
PT	The Tax and Customs Authority (AT), the Development and Cohesion Agency (AD&C), and the Institute for Agricultural and Fisheries Financing (IFAP)
LV	AFCOS network institutions, including EU Funds managing authorities (and intermediate bodies), Paying agency for EU funds for agricultural and rural development, law enforcement authorities.
DK	<p>The members of the Danish AFCOS, i.e.:</p> <ul style="list-style-type: none"> <li>• The Agency for Green Land Conversion and Water Environment</li> <li>• The Agricultural and Fisheries Agency</li> <li>• The Business Authority</li> <li>• The Ministry of Taxation</li> </ul> <p>o Incl. The Tax Agency and The Customs Agency</p> <ul style="list-style-type: none"> <li>• The Special Crime Unit (NSK)</li> </ul>

Member State	Response
IT	<p>Department for European Affairs at the Prime Minister's Office;</p> <ul style="list-style-type: none"> <li>- Department for Cohesion Policy and Southern Italy at the Prime Minister's Office;</li> <li>- Department of Public Administration at the Prime Minister's Office;</li> <li>- Department for Regional Affairs and Autonomies at the Prime Minister's Office;</li> <li>- NRRP Unit at the Prime Minister's Office;</li> <li>- Special Economic Zones (SEZ) Unit at the Prime Minister's Office;</li> <li>- Italian Court of Auditors;</li> <li>- Network of NRRP Anti-Fraud Contact Persons at the State General Accounting Department;</li> <li>- Coordination Committee for High-Level Oversight of Priority Infrastructure and Construction Projects (CCASIIP);</li> <li>- Carabinieri;</li> <li>- Guardia di Finanza;</li> <li>- National Anti-Corruption Authority (ANAC);</li> <li>- Financial Intelligence Unit (FIU) at the Bank of Italy;</li> <li>- National Anti-Mafia and Anti-Terrorism Directorate;</li> <li>- Central Criminal Police Directorate;</li> <li>- Anti-Mafia Investigation Directorate;</li> <li>- Ministry of the Interior;</li> <li>- Ministry of Justice;</li> <li>- Ministry of Economic Affairs and Finance;</li> <li>- Ministry of Enterprises and Made in Italy;</li> <li>- Ministry of Agriculture, Food Sovereignty and Forestry;</li> <li>- Ministry of Infrastructure and Transport;</li> <li>- Ministry of Labour and Social Policy;</li> <li>- Ministry of Education and Merit;</li> <li>- Customs and Monopolies Agency;</li> <li>- Revenue Agency;</li> <li>- Agricultural Payments Agency (AGEA);</li> </ul> <p>Joint Conference.</p>

**Q.4.2** How could we improve this questionnaire? Please share any suggestions for enhancements or specific areas that could be improved for future iterations.

Member State	Response
IE	n/a
LU	Important to provide the possibility for answers that are not mutually exclusive to include different statements from involved stakeholders. The way the questionnaire is structured, it does not enable opposing statements by stakeholders; mutually exclusive options are not a good tool where a variety of stakeholders with different feedback is involved.
HR	EUSurvey web page and follow-up questionnaire is structured in a way that one can provide only unified answers. Namely, we usually ask several national administrations (authorities) for the contribution to the Questionnaire, but „EUSurvey“ web page is structured in a way that one can

Member State	Response
	<p>provide only unified answers without possibility to provide other types of answers.</p> <p>For example, first question is „Have you reviewed the effectiveness of your reporting in the Irregularity Management System (IMS) in 2024?“ and it is possible that one national administration (authority) answers YES, and other answers NO. In that case, different options of answering appears. So maybe you should consider possibility of making space within the questionnaire so to be able to add different types of answers.</p> <p>In addition, in relation to some questions we would like to add certain explanations in order to better clarify the answers provided so more space would be appreciated.</p>
SE	The questions in the form should be better adapted to the administrative arrangements of the Member States. At present, it is difficult for individual managing authorities to answer questions that presuppose central governance on substantive issues that do not exist in Sweden.
NL	N/A
FR	x
EL	With the help of the competent national authorities, this questionnaire brings together data from all the Member States, thereby optimising the contribution of all recent institutional, administrative, organisational and operational developments to the defence of the economic interests of both the Member States themselves and of the European Union as a whole. Any comments/suggestions for improvement have been set out in detail in question 2.32.
BE	/
AT	No information.
FI	-
LT	-
SI	Concerns specifically in the 2.6, 2.8 and 2.9: Answers from FARS are inserted. While answers from State Prosecutors office cannot be inserted, although they are different from FARS answers. System does not allow different answers in the same line. It is not possible to mark two circles, it allows only one marking in one line.
CZ	<p>One of the entities mentioned the length of the questionnaire (22 pages). The questionnaire should be optimised in order to reduce the number of questions and to provide guidance on answering any unclear questions. Terms and concepts should be further explained.</p> <p>The type of checkboxes (one-only/multiple) in the word document in national language, which is distributed to the respondents, differs from those in the website questionnaire which is an unwelcome surprise requiring modification of several replies at the very final stage of filling-in the questionnaire.</p>
ES	No suggestions
HU	Protection of the EU's financial interests affects an increasing number of policy sectors and thus an increasing number of areas, with the result that the rules of the Member States and the related institutional set-up have been adapted to these specificities with different tasks, mandates and operational environments. In order to provide an accurate picture of the Member States on the basis

Member State	Response
	of the replies to the follow-up report, we consider it important to provide for separate answers at least on the expenditure and revenue sides of the budget for topics that can be interpreted across several EU policies, as certain questions may vary considerably depending on the field the question addresses.
SK	X
PL	<p>The anti-fraud system in Poland consists of a number of independent but cooperating institutions and bodies, including law enforcement authorities. The competent authorities of the management and control system have their own mechanisms on the basis of which they carry out their mission, including the fight against fraud, which may differ in terms of their development or implementation stage. At the same time, the questions contained in this Follow-up Questionnaire (as in the Article 325 Questionnaire) are addressed to each of the Member States individually. Similarly, the answers expected by the Commission should represent a national position (from the point of view of the Member State as a whole).</p> <p>The specific requirements of working with these questionnaires therefore necessitate some harmonisation and compromises in the manner of presenting answers. It is necessary to consult a number of relevant institutions at times, as well as to select information that jointly translates into the single ‘national’ answer in the broadest sense and to present it in a synthetic form, which is often the result of the space restrictions in the online form. This should always be taken into account by the Commission when interpreting the replies received from Member States in these questionnaires. A technical point worth mentioning is that one would expect the editable form to function better (it is a Word file generated by the system): making a choice by selecting an item from a multiple- or single-choice list or filling in specific text fields should be possible without running into technical problems. This is particularly true for the Article 325 Questionnaire form – the Word file is very badly developed from a technical point of view. In view of the need to use it in broad national-level consultations at the stage of preparing answers for the Commission, the unstable behaviour of the file makes working with it very difficult.</p>
DE	<p>The Federal Ministry of Food and Agriculture (BMEL): More targeted questions, taking into account the management and control systems in each Member State.</p> <p>The Rhineland-Palatinate ERDF Managing Authority: You could give more “not applicable/cannot assess” options for the questionnaire on topics about practices/plans on a national level. In a federal state, managing authorities do not always have knowledge about the plans on a federal level.</p>
BG	N/A
MT	The questionnaire is very detailed as it is.
CY	The questions on Arachne tool focus on the integration rather than the use of the tool, lack of integration starts from the Commission side and the tool is unable to be integrated at the moment. Arachne only works through uploading of XML files at the moment.
EE	It is difficult to give nationwide answers to such detailed questions. Institutions have different tasks, and they are at different stages of development. To ensure comparability, please distinguish topics for different institutions (investigative-, implementing institutions etc.).
RO	N/A

<b>Member State</b>	<b>Response</b>
PT	Earlier dissemination of the questionnaire
LV	The questionnaire is well prepared.
DK	Nothing to report.