



Brussels, 28 July 2026
(OR. en)

12260/26
ADD 4

GAF 36
FIN 1126

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	28 July 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union

No. Cion doc.:	SWD(2026) 248 final
Subject:	Commission staff working document: Follow-up by Member States to the Recommendations of the PIF Report 2024 accompanying the document "Report from the Commission to the Council and the European Parliament: 37th Annual Report on the protection of the European Union's financial interests and the fight against fraud - 2025"

Delegations will find attached document SWD(2026) 248 final.

Encl.: SWD(2026) 248 final



EUROPEAN
COMMISSION

Brussels, 28.7.2026
SWD(2026) 248 final

COMMISSION STAFF WORKING DOCUMENT

Follow-up by Member States to the Recommendations of the PIF Report 2024

Accompanying the document

REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

**37th Annual Report on the protection of the European Union's financial interests and
the fight against fraud - 2025**

{COM(2026) 411 final} - {SWD(2026) 245 final} - {SWD(2026) 246 final} -
{SWD(2026) 247 final} - {SWD(2026) 249 final} - {SWD(2026) 250 final} -
{SWD(2026) 251 final}

Table of Contents

1.	Overview of Member States' replies to the questionnaire.....	5
1.1.	Introduction.....	5
1.1.1.	Overarching Themes and Guiding Principle.....	5
1.2.	Recommendation 1	6
1.2.1.	Reporting maturity and strategic focus	6
1.2.2.	Best Practices	9
1.3.	Recommendation 2	10
1.3.1.	Information flow	10
1.3.2.	Cooperation between administrative and investigative/judicial bodies	11
1.3.3.	Best Practices	13
1.4.	Recommendation 4:	14
1.4.1.	Digitalisation and AI.....	14
1.4.2.	Digitalisation barriers.....	15
1.4.3.	State of Play of Arachne	16
1.4.4.	Best Practices	18
2.	Responses from the Member States	19
Q.1.1	How would you evaluate your level of maturity of your current reporting process for reporting irregularities and, in particular, fraud?.....	19
	Following Q1.1, please specify "Other".	19
Q.1.2	Which part of the Anti-Fraud Cycle do your Anti-Fraud Efforts target most?	20
Q.1.3	Please explain your reasons for this focus.	20
Q.1.4	Which part of the Anti-Fraud Cycle do your Anti-Fraud Efforts target most?	28
Q.1.5	Please explain your reasons for this choice	28
Q.1.6	How do you measure the effectiveness of your Anti-Fraud system?	34
Q.1.7	(IMS users) How do you ensure adequate knowledge of existing staff?	41
	Following Q1.7, please specify "Other".	42
Q.1.8	(IMS users) How is new staff trained on existing reporting and coordination procedures related to IMS?	43
	Following Q.1.8, please specify "Other".	44
Q.2.1	(AFCOS) What systems/practices do you have in place to ensure uninhibited information flow between judicial and reporting authorities?	46
Q.2.2	(AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? IMS	51
Q.2.2	(AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? Secure data exchange platforms (Online)	52
Q.2.2	(AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? Shared case management systems	52
Q.2.2	(AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? Encrypted email	53
Q.2.2	(AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? Regular meetings	53
Q.2.2	(AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? Other (please specify)	53
	Following Q.2.2, please specify "Other".	54
Q.2.3	(All entities involved with fraudulent irregularities) If your Member State uses secured online platforms or shared case management systems, roughly, what percentage of fraudulent	

irregularity cases are processed and followed up primarily through these digital channels (as opposed to paper or conventional correspondence)?	54
Q.2.4 (IMS users) Which IMS fields prove the most difficult to receive accurate, complete, and timely information for?	55
Q.2.5 (All entities involved with fraudulent irregularities) How do you try to balance the confidentiality of investigations with the necessity to report?	58
Q.2.6 (AFCOS) How does your system enable timely follow-up to cases in IMS?	63
Q.2.7 (AFCOS) In which areas of reporting have you encountered problems when creating or updating cases? Cooperation with national administrative bodies.....	66
Q.2.7 (AFCOS) In which areas of reporting have you encountered problems when creating or updating cases? Cooperation with national investigative bodies	67
Q.2.7 (AFCOS) In which areas of reporting have you encountered problems when creating or updating cases? Cooperation with international administrative bodies	67
Q.2.7 (AFCOS) In which areas of reporting have you encountered problems when creating or updating cases? Cooperation with international investigative bodies.....	68
Q.2.7 (AFCOS) In which areas of reporting have you encountered problems when creating or updating cases? Other (please specify)	68
Following Q2.7, please specify "Other".	68
Q.2.8 (AFCOS) Please feel free to share any additional thoughts or experiences you have regarding the topics discussed in this section or support you require from the Commission/OLAF regarding them.	69
Q.4.1 Are there any AI tools that you use as part of your national anti-fraud strategy or AFS to protect the financial interests of the Union?	72
Q.4.2 Please specify which AI tools you use as part of your NAFS?	72
Q.4.3 Please specify which AI tools you use as part of other AFS? Which AFS are they a part of?	73
Q.4.4 (AI users) What are the main uses of Artificial Intelligence within your systems?	74
Please specify "Other" uses.	74
Q.4.5. Have you conducted a cyber/AI threat assessment in 2025?	75
Q.4.6 What were the main findings of the threat assessment?.....	76
DISCLAIMER ON ARACHNE	78
Q.4.7 What is your Arachne integration status?	79
Q.4.8 If you are only partially feeding data into Arachne, what are the reasons?	79
Please specify "Other" reasons.	79
Q.4.9 For which funds is Arachne currently implemented?	80
Please specify other national or EU-funded programmes.....	81
Q.4.10 How would you describe the level of implementation across these funds.	82
Q.4.11 Are there any AI tools you use that would benefit from accessing the data available in Arachne or that could improve Arachne's performance, adoption rate by national authorities or effectiveness?.....	83
Q.4.12 When using Arachne, what are the main challenges that you face?	84
Please specify "Other" challenges.	85
Q.4.13 Has Arachne been incorporated into your NAFS or other AFS?	86
Q.4.14 Are your data analysis tools interacting with Arachne?.....	86
Q.4.15 Please list the data analysis tools which are/are planned to interact with Arachne	87
Q.4.16 How would you rate the interoperability of the systems on average?.....	88
Q.4.17 Please explain the interaction of the two (or more) systems in your administration.....	88
Q.4.18 Are you satisfied with the type of support available on Arachne?.....	89
Q.4.19 What type of support (training/content/guidebooks) on Arachne would be the most useful to you?	89
Please specify "Other" type of support.	90

Q.4.20 How do you plan to (further) incorporate digitalisation into your (future) national anti-fraud strategies?	90
Q.4.21 Please select three barriers to the digitalisation of your anti-fraud efforts, that you believe are most crucial to overcome.	93
Q.4.22 Please feel free to specify any other additional challenges or experiences regarding this section, which you would like to share.	93
Q.5.1 Please list the national services and bodies consulted to reply to this questionnaire.	94

LIST OF ABBREVIATIONS

AFA	Anti-Fraud Architecture
AFIS	Anti-Fraud Information System
AI	Artificial Intelligence
AMIF	Asylum, Migration and Integration Fund
AMLA	Authority for Anti-Money Laundering and Countering the Financing of Terrorism
AFCOS	Anti-Fraud Coordination Services
CAFS	Commission Anti-Fraud Strategy
CAP	Common Agricultural Policy
COCOLAF	Advisory Committee for the Coordination of Fraud Prevention
CONT	Committee on Budgetary Control
CSP	CAP Strategic Plan
ECA	European Court of Auditors
EDES	Early Detection and Exclusion System
EPPO	European Public Prosecutor's Office
ERDF	European Regional and Development Fund
ESF	European Social Fund
EU	European Union
FEAD	Fund for European Aid to the Most Deprived
FPDNet	Fraud Prevention and Detection Network
IBOA	Institutions, Bodies, Offices and Agencies
IMS	Irregularity Management System
IPA	Instrument for Pre-Accession
IT	Information Technology
JCO	Joint Customs Operation
JTF	Just Transition Fund
NAFS	National Anti-Fraud Strategies
OLAF	European Anti-Fraud Office
PIF	Protection of financial interests
PFIU audits	Audits on the protection of the financial interests of the Union
RRF	Recovery and Resilience Facility
RRP	National Recovery and Resilience Plan
TFEU	Treaty on the Functioning of the European Union
TOR	Traditional own resources
UAFB	Union Anti-Fraud Programme
VAT	Value Added Tax

1. OVERVIEW OF MEMBER STATES' REPLIES TO THE QUESTIONNAIRE

1.1. Introduction

In its PIF Report 2024 the Commission made recommendations to Member States, covering: a) closing the reporting gap in relation to suspected fraud and irregularities, b) establishing more effective communication channels, c) adoption of a national anti-fraud strategy, and d) digitalisation as a pillar of the national anti-fraud strategy. 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 part provides an overview and analysis of their replies, while the second part details, for each question of the survey, the specific replies given.

The replies to the third recommendation on the adoption of a national anti-fraud strategy are covered in the staff-working document on national anti-fraud strategies.

1.1.1. Overarching Themes and Guiding Principle

Similar to the previous year, three central themes emerged from the Member States' responses. First, as was the case last year, there is a strong call for training and guidance in the replies, as well as an appreciation for it. Second, Member States openly share their approaches when tackling issues such as the closing of the reporting gap. From these contributions, best practices could be formed. Where applicable, the analysis compiles best practices that Member States identified in addressing common issues to provide an overview of potential solutions. Third, there were findings in this year's replies that complement or contrast findings from last year's replies. Where applicable a comparison between findings from last year and this year is drawn.

1.2. Recommendation 1

RECOMMENDATION 1 – CLOSING THE REPORTING GAP IN RELATION TO SUSPECTED FRAUD AND IRREGULARITIES

Member States are reminded of the need to report all irregularities and suspected fraud to the Commission in a timely and complete manner in accordance with the obligations set down in sectoral regulations. This will provide for a more complete dataset at EU level facilitating better trend analysis and more timely prevention and investigation interventions

1.2.1. Reporting maturity and strategic focus

Following the 2023 PIF Report, 11 ⁽¹⁾ Member States reported having a well-established reporting system with no identified gaps. Following the 2024 PIF Report, this number rose to 18 ⁽²⁾ Member States, representing an increase of more than 60 % compared with the previous year. This may point to improvements in national reporting arrangements, greater awareness of reporting obligations, or increased confidence in national systems. At the same time, the findings should be interpreted with appropriate caution, as it is based on Member States' own assessments.

Prevention continues to be the dominant focus of national anti-fraud efforts, followed by detection. A total of 24 ⁽³⁾ Member States identified prevention as the part of the anti-fraud cycle they target most, while a remaining 3 selected detection ⁽⁴⁾. The explanations provided were highly consistent. Prevention is generally seen as more cost-effective, less administratively burdensome, and better suited to protecting EU funds before financial losses occur. Many authorities described prevention as being present in fraud risk assessments, staff training, declarations on conflicts of interest, guidance for beneficiaries, the use of red flags, early controls, and the use of Arachne.

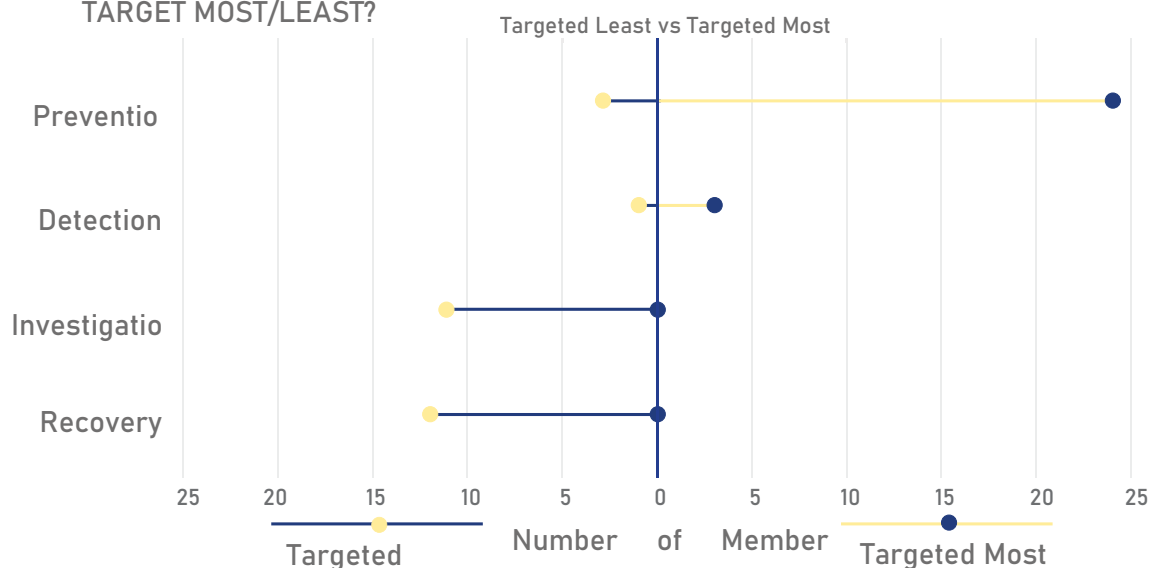
⁽¹⁾ Austria, Czechia, Estonia, Finland, France, Germany, Luxembourg, Malta, Poland, Romania, Slovakia

⁽²⁾ Austria, Bulgaria, Czechia, Germany, Estonia, Finland, Croatia, Italy, Lithuania, Luxembourg, Latvia, Malta, Netherlands, Poland, Portugal, Sweden, Slovenia, Slovakia

⁽³⁾ Austria, Belgium, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden

⁽⁴⁾ Several Member States indicated in their explanations that detection was equally prioritised, or only slightly less prioritised, than prevention.

FIGURE 1 – WHICH PART OF THE ANTI-FRAUD CYCLE DO YOUR ANTI-FRAUD EFFORTS TARGET MOST/LEAST?



By contrast, responses were more dispersed when Member States were asked which part of the anti-fraud cycle is targeted least. Recovery, investigation and detection were all mentioned. However, the qualitative replies reveal a clear pattern: investigation is often the least targeted area because it usually falls outside the remit of managing and reporting authorities and lies primarily with prosecutors, police, the European Public Prosecutor's Office (EPPO), or other judicial bodies. This was explicitly noted by several Member States, including Luxembourg, Slovenia, Czechia, Greece, Germany and Romania. Recovery was also frequently identified as receiving comparatively less attention in cases where preventive systems are already well developed and reimbursement mechanisms are firmly established.

As regards staff knowledge and training on Irregularity Management System (IMS), a clear majority of Member States rely on OLAF or Commission materials (22 Member States ⁽⁵⁾), regular training sessions (20 Member States ⁽⁶⁾), liaison officers or trainers in contact with OLAF (18 Member States ⁽⁷⁾), and national guidance or manuals (17 Member States ⁽⁸⁾).

For the training of new staff, the most commonly reported methods are: clear task allocation (19 Member States ⁽⁹⁾), national-level coordination (17 Member States ⁽¹⁰⁾), written documentation (16

⁽⁵⁾ Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Germany, Greece, Hungary, Ireland, Italy, Latvia, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Finland

⁽⁶⁾ Austria, Belgium, Bulgaria, Croatia, Czech Republic, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Romania, Slovenia, Spain, Sweden

⁽⁷⁾ Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Finland, France, Germany, Hungary, Ireland, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Croatia

⁽⁸⁾ Belgium, Bulgaria, Croatia, Czech Republic, Denmark, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Poland, Romania, Slovakia, Slovenia, Spain

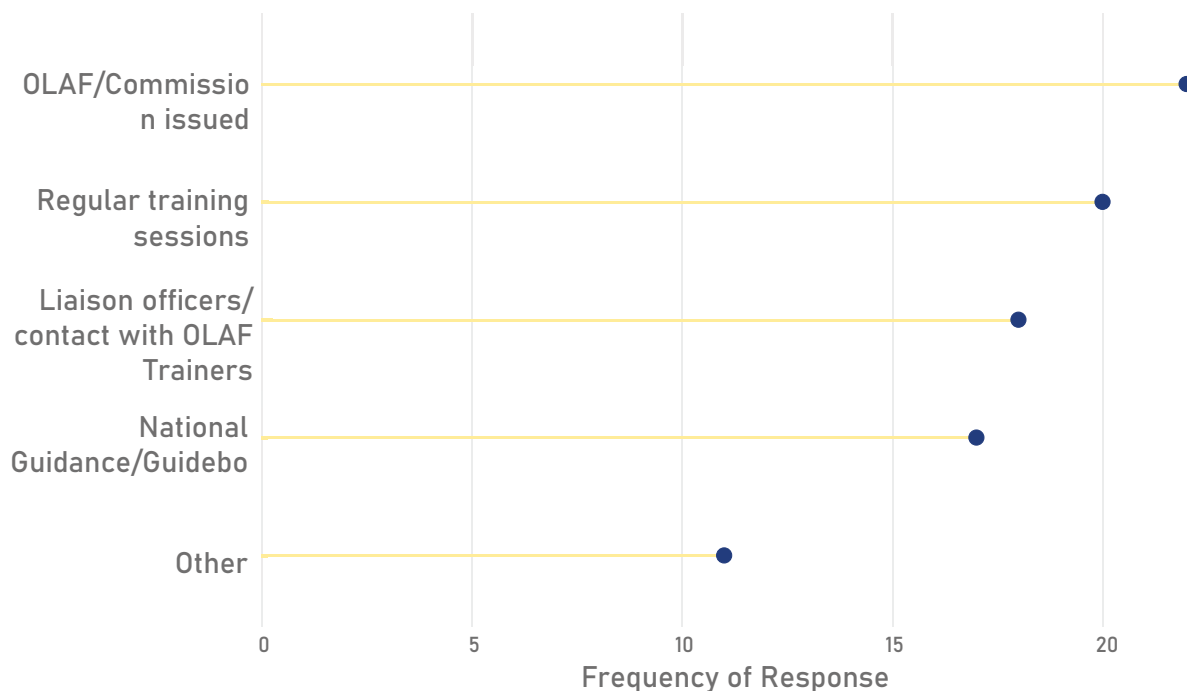
⁽⁹⁾ Austria, Bulgaria, Croatia, Czech Republic, France, Germany, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovenia, Spain, Sweden

⁽¹⁰⁾ Austria, Bulgaria, Cyprus, Czech Republic, Estonia, Germany, Hungary, Ireland, Italy, Luxembourg, Poland, Portugal, Romania, Slovenia, Spain, Sweden, Croatia

Member States ⁽¹¹⁾), and national IMS guidance (16 Member States ⁽¹²⁾). By contrast, regional-level coordination, grace periods, and coordination with other Member States are used only to a limited extent, with no more than 7 Member States reporting the use of any of these methods ⁽¹³⁾.

Overall, the replies point to a broad commitment among Member States to anti-fraud reporting, characterised by a prevention-led approach, extensive use of training, growing reliance on risk assessment, and increasing coordination through AFCOS and IMS support structures. They also suggest that closing the reporting gap depends not only on legal obligations, but equally on operational consistency, staff capacity, coordination, and systematic quality control of reporting data.

FIGURE 2 – HOW DO YOU ENSURE ADEQUATE KNOWLEDGE OF EXISTING STAFF?



⁽¹¹⁾ Bulgaria, Croatia, Czech Republic, Denmark, Finland, Germany, Ireland, Latvia, Luxembourg, Netherlands, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden

⁽¹²⁾ Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Germany, Greece, Hungary, Ireland, Italy, Latvia, Luxembourg, Poland, Slovakia, Slovenia, Spain

⁽¹³⁾ Grace Period: Belgium, Germany, Croatia, Ireland, Luxembourg, Slovenia, Slovakia

Coordination at Regional level: Austria, Germany, Spain, Ireland, Lithuania, Poland

Transfer of the case responsibility ownership: Belgium, Denmark, Croatia, Ireland, Luxembourg

Coordination with other Member States: Austria, Czechia, Croatia, Ireland

1.2.2. Best Practices

The replies show broad Member States' commitment to anti-fraud reporting, with prevention-led systems, strong use of training, growing use of risk assessment and increasing coordination through AFCOS/IMS support structures. The most transferable best practices mentioned by Member States include:

- **regular fraud risk self-assessment linked to action,**
- **strong staff training and onboarding for IMS/reporting,**
- **clear task allocation and referral pathways,**
- **use of red flags, data tools and integrated checks,**
- **national coordination mechanisms and working groups,**
- **effectiveness measurement combining audits, risks, cases and recoveries.**

The main common learning is that closing the reporting gap requires not just a legal obligation, but operational consistency, staff capability, coordination and systematic quality control of reporting data.

1.3. Recommendation 2

RECOMMENDATION 2 – ESTABLISHING MORE EFFECTIVE COMMUNICATION CHANNELS

Better coordination between national authorities, OLAF and the EPPO is also necessary to ensure that cases investigated by EU bodies are duly reported at the earliest possible moment in compliance with the relevant EU sectoral legislation. National authorities must correctly identify and address existing loopholes in the information flow in relation to suspected fraud, the moment they are first reported, and even more so, when following-up on them both in judicial and administrative proceedings at national level. The Commission is committed to further developing and providing the necessary guidelines, IT tools and support. The Commission will also facilitate to the maximum extent possible the necessary coordination between the bodies involved.

1.3.1. Information flow

The replies show that most Member States have put in place formal or semi-formal arrangements to support the flow of information between reporting and judicial authorities. These arrangements include central contact points or single points of contact, reporting guidelines and manuals, cooperation protocols or memoranda of understanding, regular inter-agency meetings, direct email exchanges, and dedicated AFCOS coordination structures.

Regular meetings are by far the most widely used coordination method, reported by 25 Member States ⁽¹⁴⁾. IMS is also widely used as a coordination tool, with 22 Member States ⁽¹⁵⁾ referring to its use in this context. Encrypted email is used by 15 Member States ⁽¹⁶⁾. It is also noteworthy that, among the 16 Member States ⁽¹⁷⁾ using either secure online platforms or shared case-management systems, 14 ⁽¹⁸⁾ rely on these tools for most of their communication

⁽¹⁴⁾ Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain

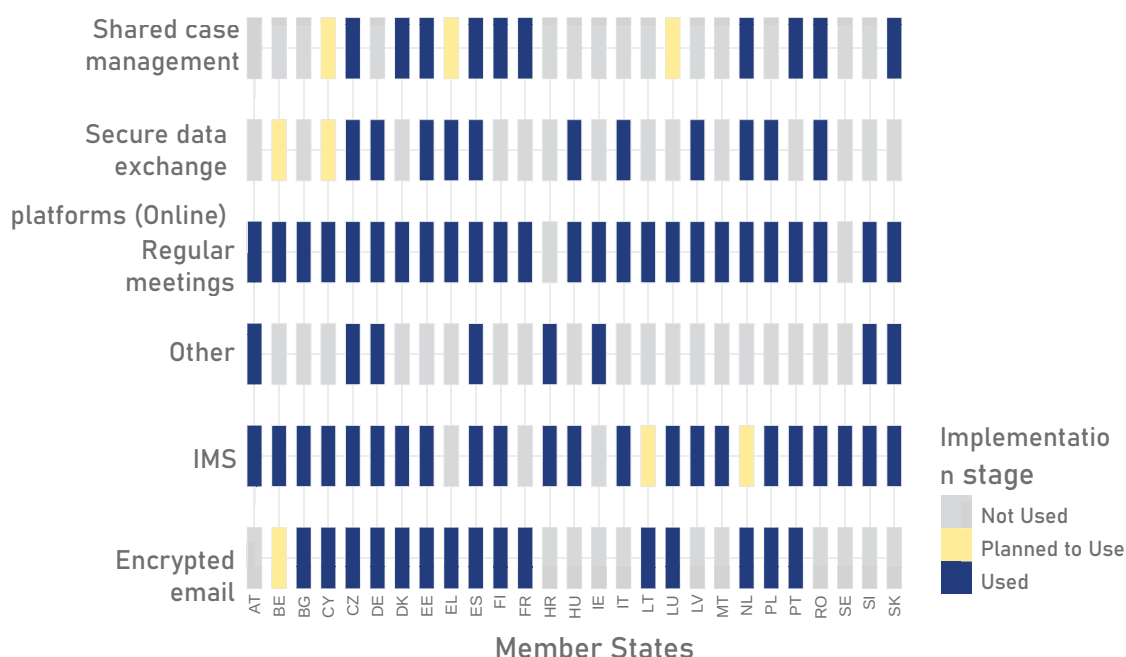
⁽¹⁵⁾ Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Germany, Hungary, Italy, Latvia, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden

⁽¹⁶⁾ Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Spain

⁽¹⁷⁾ Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Netherlands, Poland, Portugal, Romania, Slovakia, Spain

⁽¹⁸⁾ Czech Republic, Estonia, Finland, Germany, Greece, Hungary, Italy, Latvia, Netherlands, Poland, Portugal, Romania, Slovakia, Spain

FIGURE 3 – WHICH COMMUNICATION METHODS ARE USED FOR COORDINATION OF YOUR ANTI-FRAUD EFFORTS?



1.3.2. Cooperation between administrative and investigative/judicial bodies

The main operational weakness identified in the replies concerns access to timely information from investigative and judicial authorities, in particular as regards updates on ongoing criminal proceedings and final judicial outcomes. Member States repeatedly referred to difficulties in obtaining the information needed to complete or update IMS entries, especially in relation to sanctions fields, case updates, the classification of fraud or suspected fraud, modus operandi, recovery and amount fields, and judicial status and outcomes.

These difficulties are particularly pronounced where reporting authorities depend on prosecutors, police, the EPPO, or courts for updates, and where criminal proceedings are lengthy or subject to confidentiality constraints. Several Member States also referred to structural limitations linked to the EPPO Regulation, under which AFCOS does not always receive operational information directly. This confirms a pattern already identified in the PIF report 2024.

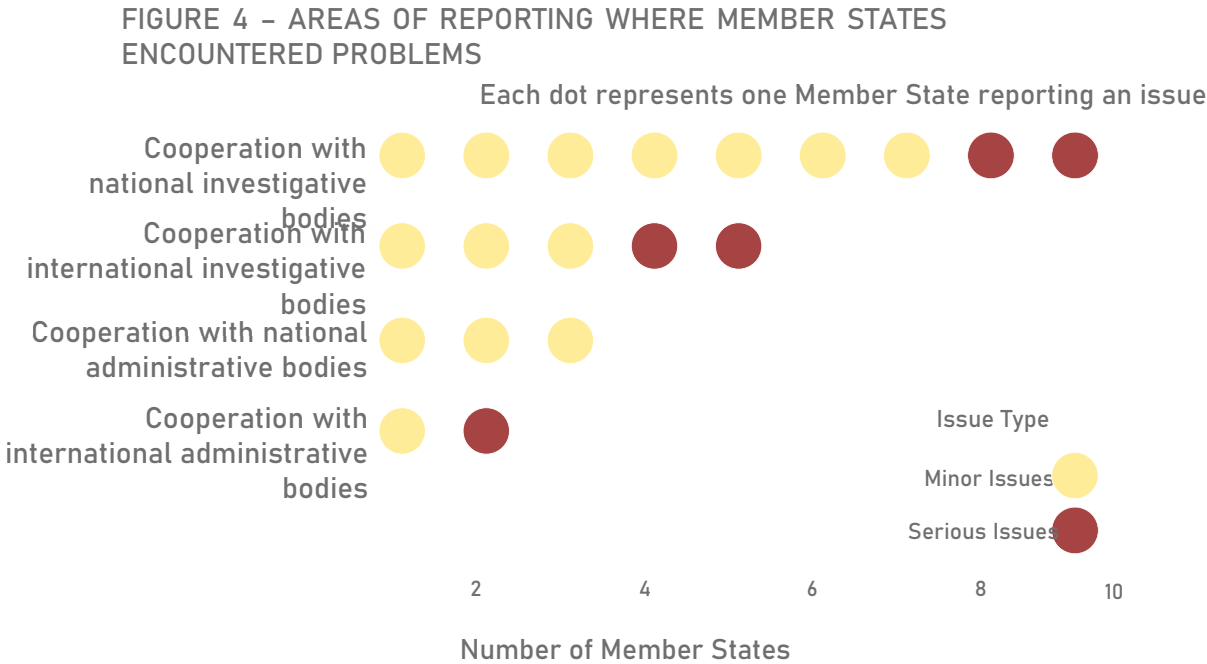
At the same time, cooperation with national administrative bodies appears to function relatively well. A total of 24 Member States ⁽¹⁹⁾ reported no issues in this area. Cooperation with investigative bodies was assessed less uniformly: 18 Member States ⁽²⁰⁾ reported no issues, 7 reported minor

⁽¹⁹⁾ Austria, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Sweden

⁽²⁰⁾ Austria, Belgium, Bulgaria, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Portugal, Romania, Slovenia, Sweden

issues ⁽²¹⁾, and 2 reported serious issues ⁽²²⁾. This suggests that the principal reporting bottleneck lies not in administrative coordination as such, but in access to follow-up information from investigative and judicial authorities once a case enters the criminal justice chain.

Taken together, the replies indicate that the effectiveness of communication channels depends less on the creation of new reporting routes than on the existence of structured governance, routine coordination, and reliable mechanisms for follow-up, particularly between administrative and judicial actors. The key challenge remains ensuring that information continues to flow after a case becomes judicial, so that administrative reporting remains timely, complete and accurate.



⁽²¹⁾ Czech Republic, Denmark, Greece, Croatia, Hungary, Poland, Slovakia

⁽²²⁾ Cyprus, Spain

1.3.3. Best Practices

The Member States' replies show that **effective communication channels depend above all on structured governance, routine coordination and reliable follow-up mechanisms**, especially between administrative and judicial actors. The most transferable best practices mentioned by Member States include:

- **formal cooperation agreements and written referral/update procedures,**
- **regular multi-authority meetings and AFCOS-led coordination,**
- **clear case ownership and periodic follow-up reviews,**
- **national case-management systems feeding into IMS,**
- **strict but workable confidentiality arrangements on a need-to-know basis and staged reporting,**
- **named contact points and liaison structures, and**
- **continuous quality control of IMS data.**

The main common learning is that improving communication is less about creating one new channel and more about ensuring that information continues to flow after a case becomes judicial, so that administrative reporting remains timely, complete and accurate.

1.4. Recommendation 4:

RECOMMENDATION 4 – DIGITALISATION AS A PILLAR OF THE NATIONAL ANTI-FRAUD STRATEGY

The Commission reiterates its call to national authorities to embed the digitalisation of the fight against fraud in their national anti-fraud strategies, with the aim of: a) assessing the level of threat posed to the EU budget by the rise in cybercrime and the use of AI and other innovative technologies, in particular by organised crime; b) identifying their knowledge and skill gaps in relation to the deployment, development and use of innovative technologies to fight fraud more effectively; c) identifying the actions needed to address such threats and vulnerabilities

1.4.1. Digitalisation and AI

Digitalisation remains an important component of anti-fraud efforts across the Member States, but implementation remains uneven and is often approached cautiously. As regards AI in particular, a large majority of Member States (21 ⁽²³⁾) reported that they do not use AI tools as part of their anti-fraud strategies. By contrast, 3 Member States ⁽²⁴⁾ stated that they use AI as part of a national anti-fraud strategy, while 6 ⁽²⁵⁾ reported using AI in the context of other anti-fraud strategies or frameworks.

Where AI is used, it is generally applied to anomaly detection and predictive analytics, reflecting the broader emphasis on prevention and detection within the anti-fraud cycle. The examples provided by Member States include AI or machine-learning tools for anomaly detection and risk analysis in agriculture and customs, tools supporting audits and the prediction of irregularities, text-processing and transcription support, analytical applications in risk scoring or network analysis, and automated invoice checks.

Overall, the replies suggest that the use of AI remains at an exploratory stage and is more often sector-specific than fully integrated into national anti-fraud systems.

The replies also indicate limited progress in the assessment of cyber- and AI-related threats. Only 3 Member States reported having carried out a comprehensive assessment in 2025, while 8 ⁽²⁶⁾ carried out a partial assessment. A further 15 Member States ⁽²⁷⁾ reported having conducted no such assessment and having no plans to do so, while 1 Member State ⁽²⁸⁾ indicated that such an assessment was planned. This suggests that the recommendation to assess cyber and AI-related threats is only beginning to be reflected in national practice.

As regards future digitalisation efforts, Member States indicated that they intend to focus in particular on stronger interoperability between systems, expanded use of Arachne and future Arachne+, improved risk-analysis tools, better data integration, possible use of AI for anomaly

⁽²³⁾ Austria, Belgium, Bulgaria, Cyprus, Denmark, Estonia, Finland, Germany, Greece, Ireland, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Romania, Slovakia, Slovenia, Sweden, Croatia

⁽²⁴⁾ Czech Republic, Italy, Portugal

⁽²⁵⁾ Belgium, France, Hungary, Italy, Slovenia, Spain

⁽²⁶⁾ Austria, Belgium, Estonia, Ireland, Latvia, Malta, Slovakia, Spain

⁽²⁷⁾ Bulgaria, Cyprus, Denmark, Finland, France, Germany, Greece, Croatia, Hungary, Lithuania, Netherlands, Poland, Portugal, Romania, Slovenia

⁽²⁸⁾ Italy

detection or complaint analysis, and digital platforms to support transparency and case management.

1.4.2. Digitalisation barriers

The previous year's analysis identified interoperability problems, legal barriers, and data protection or security concerns as the main obstacles to further digitalisation. This year's replies confirm the same barriers and allow them to be quantified more clearly. The three most significant barriers identified by Member States are interoperability challenges (19 Member States ⁽²⁹⁾), budget constraints (16 Member States ⁽³⁰⁾), and data-protection concerns or other legal issues (12 Member States ⁽³¹⁾).

These findings suggest that the main obstacles to further digitalisation are structural and organisational, rather than conceptual. The qualitative replies reinforce this conclusion. Member States referred to systems that do not communicate effectively with one another, uneven data quality and access, fragmented institutional arrangements that slow digital progress, legal and privacy frameworks that complicate automated data use, and existing applications that are rigid and costly to adapt.

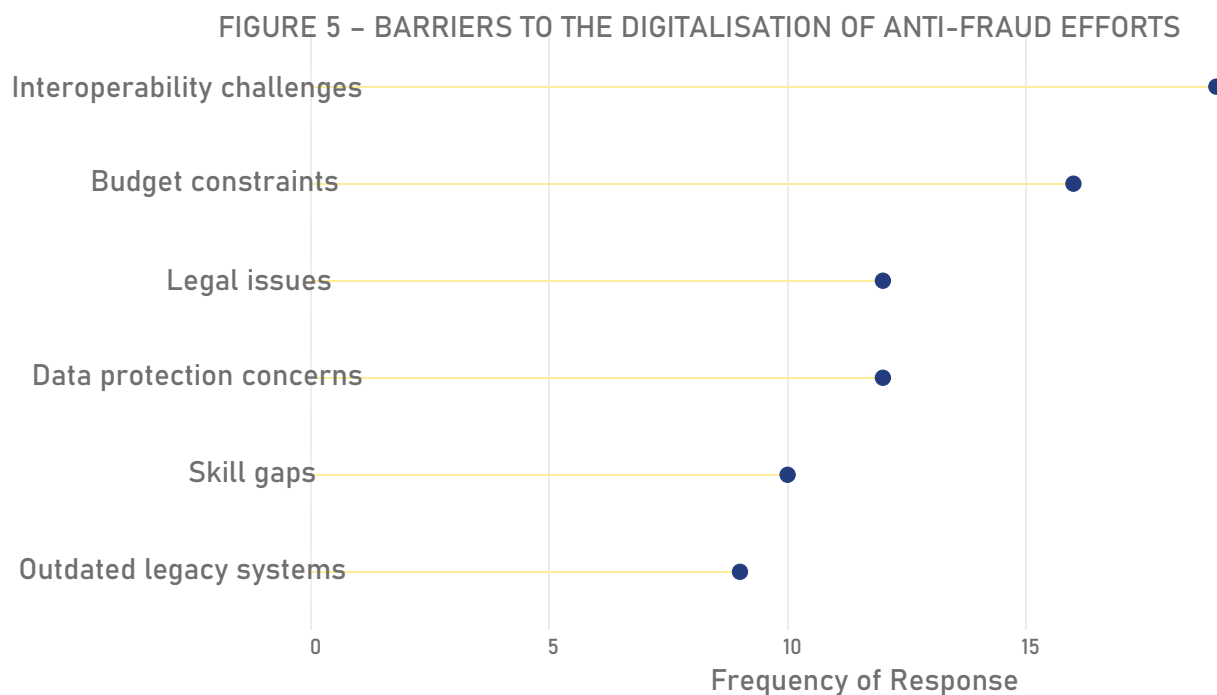
Member States that are more advanced in this area emphasised, in particular, the need for interoperability, common data standards, and stronger support from the Commission and OLAF.

⁽²⁹⁾ Cyprus, Estonia, Finland, France, Germany, Greece, Croatia, Hungary, Ireland, Italy, Latvia, Luxembourg, Malta, Netherlands, Portugal, Slovakia, Slovenia, Spain, Sweden

⁽³⁰⁾ Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Poland, Romania, Slovakia, Spain, Croatia

⁽³¹⁾ Data protection concerns: Austria, Belgium, France, Germany, Greece, Hungary, Ireland, Luxembourg, Malta, Poland, Portugal, Sweden

Legal issues: Austria, Bulgaria, Cyprus, Czech Republic, Estonia, France, Germany, Lithuania, Poland, Romania, Slovakia, Sweden



1.4.3. State of Play of Arachne

Last year’s analysis found that 22 Member States ⁽³²⁾ used Arachne as part of their anti-fraud strategies. This year, that number has risen slightly to 23 ⁽³³⁾. At the same time, the survey provides a more nuanced picture of how the tool is implemented in practice. Arachne is not simply either “used” or “not used”. In many cases, it is only partially integrated: data may cover only certain funds, be uploaded manually, or be provided only to a limited extent. The findings therefore point not only to broad uptake of the tool, but also to considerable variation in the depth and quality of its use.

The main reasons cited by Member States for partial implementation are technical limitations (8 Member States ⁽³⁴⁾), strategic decisions to provide only the minimum dataset (7 Member States ⁽³⁵⁾), and legal constraints (6 Member States ⁽³⁶⁾). This suggests that partial integration is often a pragmatic compromise rather than a rejection of the tool itself.

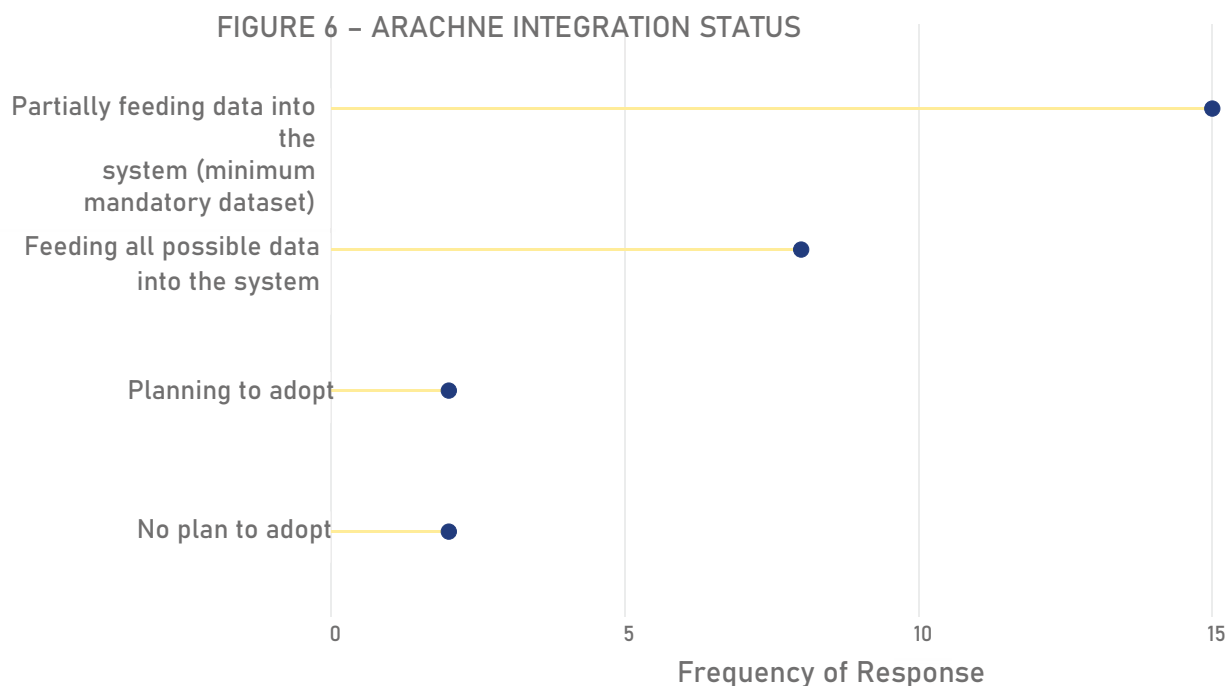
⁽³²⁾ Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Estonia, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain

⁽³³⁾ Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Croatia, Hungary, Ireland, Italy, Latvia, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain

⁽³⁴⁾ Cyprus, Czech Republic, France, Greece, Ireland, Luxembourg, Slovenia, Spain

⁽³⁵⁾ Czech Republic, Finland, France, Latvia, Luxembourg, Slovenia, Spain

⁽³⁶⁾ Austria, Cyprus, France, Poland, Slovenia, Spain



Problems already identified by individual Member States in the last year's questionnaire were confirmed by the replies to this year's targeted questions. The most frequently cited obstacles to wider use or deeper implementation of Arachne are false alerts (19 Member States ⁽³⁷⁾), difficulty in interpreting indicators (18 Member States ⁽³⁸⁾), and compatibility issues (14 Member States ⁽³⁹⁾). The individual replies also reveal additional recurring concerns, including the lack of unique identifiers for individuals, the absence of automatic access to certain national data, unclear audit trails or source data, unclear algorithms, and the time-consuming nature of manual uploads.

According to Member States, these factors also help explain why interaction between Arachne and other national data-analysis tools remains limited. Where such interaction exists, interoperability is generally assessed as medium to high, but the number of Member States concerned remains small. In practice, many systems still rely on XML exports, manual uploads, or extraction from national systems into Arachne, rather than on automated or API-based interoperability.

Views on the support available for Arachne are mixed. Nine Member States reported being satisfied with the support provided, and also nine reported dissatisfaction. The most frequently requested forms of support are staff training (13 Member States ⁽⁴⁰⁾), Arachne Academy tutorials and videos (12 Member States ⁽⁴¹⁾), and guidance on risk indicators and their interpretation (12 Member

⁽³⁷⁾ Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, France, Greece, Croatia, Hungary, Italy, Latvia, Luxembourg, Malta, Poland, Portugal, Slovakia, Slovenia, Spain

⁽³⁸⁾ Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, France, Greece, Croatia, Hungary, Ireland, Italy, Latvia, Portugal, Romania, Slovakia, Slovenia, Spain

⁽³⁹⁾ Austria, Belgium, Czech Republic, Finland, France, Hungary, Ireland, Italy, Luxembourg, Poland, Portugal, Slovakia, Slovenia, Spain

⁽⁴⁰⁾ Belgium, Bulgaria, Czech Republic, France, Greece, Croatia, Hungary, Luxembourg, Poland, Romania, Slovakia, Slovenia, Spain

⁽⁴¹⁾ Belgium, Bulgaria, Czech Republic, Greece, Croatia, Hungary, Luxembourg, Poland, Romania, Slovakia, Slovenia, Spain

States ⁽⁴²⁾). This again underlines a broader pattern in the replies: the challenge lies not only in access to the tool, but also in ensuring that its outputs are sufficiently clear, usable, and operationally relevant.

1.4.4. Best Practices

The replies show that Member States increasingly recognise digitalisation as an essential pillar of anti-fraud policy, but implementation remains uneven, fragmented and constrained by interoperability, legal uncertainty and limited budget. The most transferable best practices mentioned by Member States are:

- **embedding digitalisation in anti-fraud strategies,**
- **improving interoperability between national systems and EU tools,**
- **deploying AI in targeted, secure and risk-based ways,**
- **combining digital outputs with human analysis and operational follow-up,**
- **clarifying legal and data protection frameworks, and**
- **investing in training and technical support.**

The main common learning is that digitalisation becomes a more effective part of anti-fraud efforts when it is backed by usable data, interoperable systems, legal certainty, skilled staff and integration into everyday control workflows.

⁽⁴²⁾ Belgium, Bulgaria, Czech Republic, France, Greece, Croatia, Hungary, Luxembourg, Romania, Slovakia, Slovenia, Spain

2. RESPONSES FROM THE MEMBER STATES

RECOMMENDATION 1 – CLOSING THE REPORTING GAP IN RELATION TO SUSPECTED FRAUD AND IRREGULARITIES

Member States are reminded of the need to report all irregularities and suspect fraud to the Commission in a timely and complete manner in accordance with the obligations set down in sectoral regulations. This will provide for a more complete dataset at EU level facilitating better trend analysis and more timely prevention and investigation interventions

Q.1.1 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	18	66.7%	AT, BG, CZ, DE, EE, FI, HR, IT, LT, LU, LV, MT, NL, PL, PT, SE, SI, SK
We are currently improving our reporting system to better capture and report suspected fraud cases and irregularities	3	11.1%	BE, EL, FR
We have a strong reporting system but with some gaps in capturing all relevant data	3	11.1%	CY, DK, HU
Other (please specify)	3	11.1%	ES, IE, RO

Following Q1.1, please specify "Other".

Member State	Response
ES	Most of the managing authorities consulted indicated that they are currently improving the reporting system, except for two authorities that use a strong or well-established reporting system.
IE	Option 2 is our choice - to add narrative to explain this: Each reporting authority in Ireland attended IMS training by OLAF in October 2025, clarifying obligations in terms of IMS. This has been revisited in interdepartmental meetings which they have all attended, Much expenditure coming from the funds under shared management funds are incurred via the Exchequer vote process before they come from the support of the EU fund. Any

Member State	Response
	instances of fraud/ suspected fraud would fall within the anti-fraud policies of the government department and would therefore be excluded from expenditure declarations.
RO	Following consultation with the bodies listed in the reply to question 5.1, it became apparent that the reporting process is at various stages of development. Consequently, multiple answers apply - specifically, the first three options.

Q.1.2 Which part of the Anti-Fraud Cycle do your Anti-Fraud Efforts target most?

Response	Frequency	Percentage	Member States
Prevention	24	88.9%	AT, BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LV, MT, NL, PL, PT, RO, SE, SI, SK
Detection	3	11.1%	BG, DK, LU

Q.1.3 Please explain your reasons for this focus.

Member State	Response
AT	BMLUK [Federal Ministry of Agriculture and Forestry, Climate and Environmental Protection, Regions and Water Management]: To increase awareness in the area of funding; compliance training at BMLUK. The other parts of the cycle are also covered, e.g. annual review by the certification body of recoveries by the paying agency. BMASGPK [Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection]: This focus is established in the anti-fraud strategy for the ESF+/JTF.
	Which part of the Anti-Fraud Cycle do your Anti-Fraud Efforts target most?
BE	BE AFCOS: Prevention is the foundation of a coherent anti-fraud approach. Thanks to our stakeholder management we have noticed that a lack of anti-fraud knowledge throughout the network. Given this reality we have restarted with the basics to improve overall levels of comprehension of the whole Anti-fraud Cycle. PSW (Public Service of Wallonia) ERDF Wallonia: The PSW emphasises the pillars of prevention and detection in that it highlights those

Member State	Response
	things that make it possible to reduce the overall risk and limit subsequent costs, since detection is an indispensable ally to prevention. The PSW emphasises the in-depth assessment of fraud risks, the implementation of preventive measures, the raising of awareness and training of staff, the reduction of fraud opportunities before they arise, early detection mechanisms, enhanced checks, and tools to alert and report. FPS (Federal Public Service) Finance (Customs disputes): The mandate of the Disputes Department is to recover duties; it therefore makes sense that their efforts are more focused on recovery than on the other strands of the anti-fraud cycle. EUROPA WSE (ESF VL): As MA we focus on detection because every organisation that receives European funds has to report. We perform checks on those reports, which lead to corrections. While there is significant focus on prevention (e.g. informing the organisations), the main body of work concerning anti-fraud happens at the reporting stage. That is also when we can sanction the organisations. Investigation and recovery concerning anti-fraud is handled by different services within our department/government. ERDF and RRF Brussels Capital Region: The use of Arachne focuses primarily on preventing and detecting fraud and irregularities. In the context of project selection, ex ante analyses are also carried out in relation to double sources of financing. The checking and analysis of the permit from the authorities also concerns detection of possible irregularities and potential conflicts of interest in order to prevent fraud. ESF Agency (ESF Wallonia-Brussels): The ESF Agency improves these procedures for detecting irregularities and fraud risks; it is part of the French Community's working group on combating fraud. As part of the renewal exercise for 2026-2027, an analysis was carried out for both the double subsidy risk and the financial risk for all the files.
BG	Prevention in the fight against irregularities and fraud is of paramount importance for protecting the EU's financial interests. Applying preventive measures reduces the risk of fraud and other irregularities. These types of measures are a more effective and efficient way of protecting financial interests than taking action after a fraud has already been committed
CY	Prevention is the primary focus of the anti-fraud cycle. Focusing on prevention helps ensure compliance with EU regulations, minimise the risk of financial corrections imposed by the European Commission, and safeguard EU and national resources. Strong prevention through risk assessments, clear procedures, guidance, and training, limits fraud risks in key areas such as public procurement and project implementation, while promoting integrity, accountability, and effective use of EU funds in Cyprus.
CZ	Prevention can lead to much greater efficiency in the use of public funds. By raising staff awareness and effectively vetting grant applicants during the evaluation phase (i.e., before the legal act is issued), many problematic applicants can be excluded at this stage, thereby preventing future cases that would otherwise require additional audits, sanctions, and enforcement actions. Prevention plays an important role in the National Recovery Plan (action plan for the systematic prevention of conflicts of interest, red-flag warning system). We consider fraud prevention to be a vital part of the cycle. If appropriate anti-fraud measures are taken, the incidence of fraud will be reduced, leading to a reduced need for subsequent detection, investigation and enforcement.

Member State	Response
DE	Prevention is an essential element of the work of the controls and irregularities unit, which focuses primarily on systematic risk prevention by means of regular staff training, specialised workshops and continuously strengthening internal control mechanisms. Other preventive measures include rigorous project checks, during which we focus on identifying potential irregularities and ensuring compliance with the rules on protecting the EU's financial interests. The objectives are to minimise the risk of fraud, increase the transparency of processes and ensure that public money is handled responsibly. Another objective is to prevent irregularities and fraud at the stage of preparation and administration of projects. Much of the work consists of setting up control procedures, internal guidelines and methodological support. Please note: There was an equal number of votes by the contributors for "Prevention" and "Detection".
	The Rhineland-Palatinate ERDF managing authority: Under administrative proceedings, the focus is on prevention and detection, given that investigation is primarily the task of the law enforcement authorities.
	The North Rhine-Westphalia (NRW) ERDF managing authority: Limiting the scope for fraud through simplified cost options and evidence requirements.
	The Saxony-Anhalt ESF managing authority: Prevention, detection and recovery are core tasks of the managing/certifying authorities. In Germany, the law enforcement authorities are responsible for investigation.
	The Lower Saxony ERDF managing authority: When fraud and corruption are detected at an early stage, the subsequent funding processes are not affected. Fraud risks are identified at an early stage through analysis and monitoring and countered through targeted measures.
	The EU Paying Agency for Lower Saxony, Bremen and Hamburg: We focus on detection and reporting cases to the public prosecutor's office and OLAF. Fraud prevention training is also provided.
	The ESF Plus Federal Programme, led by the Federal Ministry of Labour and Social Affairs (BMAS): The focus is on prevention and detection for preventive and efficiency-related reasons. Consequently, the number of cases of fraud or suspected fraud can be reduced from the outset in a pre-emptive manner, meaning there is naturally less need for investigation and recovery.
	The Schleswig-Holstein ERDF managing authority: In principle, prevention reduces risks, which means that the amount of work in terms of detection, investigation and recovery is lower in the first place.
	The Bremen ERDF managing authority: Identifying possible intentions of fraud is a prerequisite for an effective anti-fraud strategy. In particular, this concerns the staff of the bodies involved in the implementation of the ERDF (intermediate bodies, managing authority, accounting body). Appropriate awareness-raising is carried out by means of training courses or mandatory instructions, which the managing authority makes available to the competent bodies.
	The AMIF managing authority: The focus is on preventing, detecting and investigating irregularities and fraud. This serves to protect the AMIF managing authority, the entire grant system and EU funds.
	The Federal Office for Agriculture and Food (BLE): Infringements identified in relation to the measures we implement are generally not

Member State	Response
	deliberate infringements committed with the intention of perpetrating fraud but negligent acts (failing to meet deadlines/submit notifications, negligently providing incorrect information, etc.). In this context it should also be noted that, under German law, intent to commit fraud must be proven. Thus, the focus is more on identifying fraud risks, raising awareness and analysing management and control systems, all of which are grouped together as a set of measures. The Hessen ERDF managing authority : Prevention and detection help stop the EU funds in question from being charged to the Commission at all. Management and control systems have a particular impact on these two stages. The Thuringia ERDF managing authority: The ERDF guidance document provides direction for the intermediate bodies on following up on suspicious transactions. It includes an annex on indicators of fraudulent or corrupt behaviour. Particularly in investigations, the managing authority helps to ensure the availability of all the information needed to determine whether there is an irregularity in the case. The Baden-Württemberg ERDF managing authority: A focus on fraud prevention can often obviate the need for further anti-fraud measures. The Brandenburg ERDF managing authority: Preventive measures to combat fraud in relation to the EU budget are generally less costly than subsequent detection and sanctioning of fraud cases. Targeted prevention makes more efficient use of public funds and avoids the costs of investigations, court proceedings and recoveries. Moreover, prevention reinforces trust in the EU, averts financial losses for the EU budget and helps stop the misuse of EU funds. Preventive checks, internal audits and risk management systems enable weaknesses in the system to be identified at an early stage and can prevent an additional burden for EU institutions.
DK	Danish Business Authority: We find it difficult to prevent fraud and don't encounter a lot of fraud cases, therefore resources are best spent on detection and investigation. Danish Agricultural and Fisheries Agency: A strong focus in our Anti-fraud system lies in case workers' identification of "Red Flags".
EE	Our anti-fraud efforts address all stages of the Anti-Fraud Cycle, as each phase is essential for a resilient system. However, our implementing authorities primary focus is on prevention — particularly on risk assessment and thorough application screening. Strengthening these early-stage controls helps us significantly reduce downstream issues, since detection, investigation, and recovery are far more resource-intensive and place a heavier burden on the system. By identifying risks upfront, we aim to minimise the likelihood that cases escalate into later, more problematic stages and thereby reduce overall system-level issues. While investigative bodies place the greatest emphasis on successfully pursuing criminal cases, implementing authorities prioritise early-stage prevention to stop issues before they develop into cases requiring investigation.
EL	'Special Service for Institutional Support and Information Systems (EYTHYPS): Addressing fraud risks in a timely manner through more robust procedures, audits and transparency mechanisms limits the likelihood of irregularities, reduces the administrative and financial costs of subsequent corrections, and more effectively ensures the correct and lawful use of EU resources. Recovery and Resilience Facility Special Coordination Service (EYSTA): The responsibilities of the Service and the other bodies involved in the planning and

Member State	Response
	implementation of Recovery and Resilience Fund (RRF) projects and actions are limited to the taking of measures to prevent and detect irregularities (including those indicating fraud) in RRF projects and to correct/recover the relevant resources from the final recipients of the funds. Investigative powers have been conferred to and are exercised by other national bodies.
ES	For management authorities, efforts are mainly focused on prevention, identifying the risks associated with different procedures and adopting various preventive measures (risk assessment, development of an anti-fraud culture, codes of ethics, staff training and awareness-raising, segregation of duties, procedures to prevent conflicts of interest) in order to prevent or significantly reduce the occurrence of fraud. They also devote considerable effort to the detection phase, with robust detection systems that complement a framework focused on preventing fraud from occurring in the first place, with detection acting as a second line of defence and prevention as the backbone of the model. Detection would complement this approach through continuous controls, administrative and technical checks in the field, early warning mechanisms and reporting channels, which make it possible to identify potential irregularities at an early stage and take action as soon as possible. A managing authority indicates that it has an anti-fraud strategy in place, which includes measures to combat fraud and any illegal activity affecting the financial interests of the Union. These measures include fraud prevention and detection, conditions for investigating fraud, and recovery and deterrence measures with proportionate and dissuasive penalties.
FI	The fight against fraud focuses on an effective and efficient management and control system for preventing fraud. Up-to-date guidance and regular training support the system and ensure it functions. These measures ensure that staff are familiar with the necessary procedures and receive practical guidance on how to apply the legislation, thereby strengthening fraud prevention and fostering a culture of responsibility.
FR	To protect the EU budget, the first step is to increase efforts to prevent fraud, focusing on three areas: - greater consideration of the risk of fraud by all bodies responsible for the management of European funds and in the context of audits; - continuation of the proactive policy pursued by partners in relation to the professionalisation of staff responsible for combating fraud; - increasing awareness of breaches of probity in risk sectors.
HR	Contribution from the Ministry of Agriculture, Forestry and Fisheries, Directorate of Fisheries: We consider prevention important as it contributes significantly to reducing the risk of irregularities and consequently reducing the number of investigations and finally of recoveries. Contribution from the Ministry of Labour, Pension System, Family and Social Policy: We target prevention and detection most since this seems to be the best way to avoid irregularities and frauds in general. Contribution from the Ministry of Regional Development and EU funds: Anti-fraud efforts within the management and control system for the use of ESI Funds target all elements of the Anti-Fraud Cycle – prevention, detection, investigation and recovery – as they are equally important for the effective protection of the EU's financial

Member State	Response
	interests. Managing Authority and other bodies in the management and control system for the use of ESI Funds are responsible for preventing and detecting irregularities and suspected fraud in a timely manner, ensuring appropriate follow-up and reporting, and monitoring the implementation of corrective measures, including financial corrections and the recovery of unduly spent funds. Contribution from the Ministry of Finance, Customs Administration: Prevention - by using the risk analysis system during the import customs clearance procedure, we use defined risk rules. Detection - refers to the post clearance control. When selecting a company for post clearance control, we apply statistical mathematical analysis. Recovery (refund) - we take all legal measures for the payment of established duties from the debtor and from the persons who guarantee such amounts (e.g. customs agent provides a guarantee for the importer). Contribution from the Ministry of Agriculture, Forestry and Fisheries (Paying Agency for Agriculture, Fisheries and Rural Development): After establishing of irregularities, Paying Agency takes the appropriate measures to remedy the deficiencies of irregularity and where appropriate, to recover the amounts wrongly paid taking into consideration all case circumstances and influence of irregularity on project eligibility. Contribution from HR AFCOS unit: From our point of view, based on the risk assessment and training needs analysis, it can be concluded that the focus is put mainly on prevention. However, this does not diminish the efforts of other bodies within the AFCOS System, whose focus is also on other parts of the Anti-Fraud Cycle.
HU	Our strategic choices were influenced by the 'prevention is better than cure' approach.
IE	Authorities in Ireland have expressed that the nature of the Exchequer funding provided upfront to fund cofinancing actions leads to prevention being targeted the most. Departments have committed to promoting cultures that deter fraudulent activity, to facilitate the prevention of fraud and corruption. This area being targeted the most does not negate measures in place to target all stages of the Anti-Fraud cycle.
IT	Measures to combat illegal conduct focus on overseeing the entire anti-fraud cycle, in order to ensure the timely detection of irregularities and fraud, thereby safeguarding the financial integrity of the EU budget. The strengthening of preventive controls, risk analysis and the coordination of investigations makes it possible to identify problems at an early stage and to take the necessary corrective action quickly. European and national funds are managed according to a number of largely binding procedures governing the various stages: beneficiaries are chosen according to established criteria; the implementation of projects by beneficiaries and the certification of expenditure are subject to first-level sample checks using an extraction methodology based on prior risk assessment. The checks are, in turn, subject to quality review procedures and are supported by a management information system in which each individual project undergoes continuous automatic checks prior to the first-level checks. The MA prepares and provides instructions to beneficiaries for the proper implementation and management of the measures; any reports of suspected irregularities or fraud in the context of the implementation of projects funded by the Programme are carefully investigated by the MA, which then takes all appropriate measures; participation in training courses on the ethics and legality of all office resources is encouraged; declarations of the absence of conflicts of interest in regard to the office's internal resources and of all those involved in the implementation of the funded projects are obtained; the Arachne risk classification system is used and periodic risk self-

Member State	Response
	assessments are carried out in accordance with the methodology indicated by the European Commission, through the Risk Self-Assessment Group (GAR), measuring the probability and impact of specific and commonly recognised risks that are particularly relevant to the Programme's key processes, with corrective action taken where the risk exceeds the accepted limit.
LT	We have noticed that we need to pay more attention to prevention, so we are talking to the Agencies, who provide financial support from European funds to do this more responsibly. Therefore, we are paying more attention to working with the Agencies.
LU	Because of the format of the answers, we chose one option, i.e. detection. However, we focus on both prevention and detection. We cofinance projects in the area of RDI and renewable energy production, as well energy efficiency. The beneficiaries have to pay every expense in advance and get then reimbursed by the ERDF, based on the checks we perform. We do not intervene in their existing accounting procedures as this would be far beyond scope and our responsibility. Before agreeing to cofinance a project, we perform checks on the reputation, financial and administrative capacities of the potential beneficiaries and verify that their financial statements have been published as well as their fiscal and social obligations are fulfilled. That would reduce the risk beforehand and could maybe be considered as prevention measure. The focus on prevention is essential to the ESF+ because it protects the integrity, resources, and long-term stability of EU funds. Strong preventive measures reduce opportunities for misconduct and ensure that public funds are used for their intended purposes. By identifying risks early, we can detect irregularities before they escalate into significant financial or reputational damage.
LV	Prevention stops the fraud before it happens, which is always more cost-effective than repairing damage afterward.
MT	This question is not applicable since prevention, detection, investigation and recovery are all dealt with by the respective national authorities accordingly. Kindly refer to the reply provided in Question 1.6.
NL	Prevention is better than cure and therefore the focus is on prevention. However, different parties approach the fight against fraud from slightly different angles. Dutch Customs (revenue) mainly manage investigations and recovery. The managing authorities (expenditure) mainly deal with prevention.
PL	In cohesion policy, prevention in the anti-fraud cycle is a key element ensuring that EU funds are used correctly, efficiently and in line with the law. In the implementation of EU funds, prevention is systemic and is an integral part of the management and control system. In accordance with Article 74 of Regulation (EU) 2021/1060, institutions are obliged to have effective and proportionate anti-fraud measures and procedures in place. This means, among other things, that they are obliged to conduct fraud risk assessment and carry out verifications to respond to emerging threats. This allows risks to be identified earlier, e.g. before grant agreements are concluded or procurement takes place. Another function of prevention in the anti-fraud cycle in cohesion policy is to protect the financial interests of the EU. In accordance with the principle of sound financial management, EU money should be spent in a way that ensures legality, efficiency and economy. Effective prevention reduces the number of financial corrections and the risk of payments being suspended and thus has a direct impact on the liquidity of programmes and beneficiaries. In addition, effective preventive mechanisms significantly reduce the likelihood of fraud, while the cost of prevention is markedly lower than that of reacting to fraud that has already happened. Prevention also makes the other stages of the anti-fraud cycle more efficient since, through transparent processes, it makes it easier for irregularities to be detected. Although detection, investigation and recovery are crucial, it is prevention that determines

Member State	Response
	the effectiveness of the entire system of protection and the fight against irregularities and fraud. In agricultural policy, the detection stage is of key importance and is facilitated by a series of effective tools that have been introduced and are used to identify potential fraud, particularly during the verification of aid applications. These tools include guidelines and entries in handbooks of procedures outlining the process of detecting atypical elements that can be an indicator of fraud.
PT	A number of fraud-prevention measures have been adopted under the National Anti-Fraud Strategy (NAFS), such as adopting anti-fraud policies, establishing mechanisms to ensure coordination between the various bodies involved in handling and monitoring European funds, and setting up integrated IT systems.
	Following consultation with the bodies listed in the reply to question 5.1, it became apparent that the answers to this question vary and are specific to the activities of each body, meaning the answer covers three parts of the anti-fraud cycle: prevention, investigation and recovery. Their detailed responses are presented below. National Agency for Public Procurement: Prevention and detection. In its capacity as reform and investment coordinator, the National Agency for Public Procurement conducts verification and control activities for projects funded under the national recovery and resilience plan in accordance with Government Emergency Order No 70/2022, which established the applicable arrangements in relation to the cycles referred to above. Ministry of Energy: Investigation. The limited number of staff involved in investigating and resolving suspected irregularities makes the prevention and detection stages difficult to implement. To remedy these deficiencies, platforms and algorithms could be created to prevent the emergence of suspicions of irregularities.
RO	Ministry of Investments and European Projects: Prevention, detection and recovery. The Managing Authority regularly implements measures to prevent and detect fraud and to recover unduly paid amounts. North-East Regional Development Agency: Prevention is a priority in our strategy in order to mitigate fraud risks and foster closer cooperation and stronger coordination among all stakeholders. Detection: the occurrence of multiple situations that arose in 2025 has highlighted the need for staff to prioritise detection and improve detection methods. West Regional Development Agency: Prevention and detection. This is the first financial cycle where the West Regional Development Agency serves as the Managing Authority for the 2021-2027 West Regional Programme. Managing Authority for the South-West Oltenia Regional Programme: Prevention, detection and recovery. The Regional Development Agency's anti-fraud efforts are focused on preventing and detecting irregularities and suspected fraud at an early stage, and on recovering affected amounts through financial corrections and administrative measures, in line with applicable legislation. These activities are carried out in line with the managing authority's role as the administrative authority responsible for managing EU funds. North-West Regional Development Agency:

Member State	Response
	As no cases of suspected fraud were identified in 2024, efforts under the anti-fraud strategy are focused on prevention and detection.
SE	Prevention is cost-effective.
SI	Reply for the AKTRP (Agency for Agricultural Markets and Rural Development): we would indicate three areas: Prevention, Detection and Recovery (since the link does not allow all three to be selected at the same time). These three areas are systematically regulated at the Agency. Each of the areas is supported by written procedures. We have a system of red flags, checklists and funding recovery procedures in place at the institution. Reply for the MKRR (Ministry of Cohesion and Regional Development), which has indicated two areas: Prevention and Detection (since the link does not allow both to be selected at the same time). As the managing authority (MA) for ESI funds, the Ministry strives, within the limits of its powers, to prevent and detect irregularities and fraud under the management and control system (MCS system) in place.
SK	Anti-fraud measures are designed to cover all stages of the anti-fraud cycle. Anti-fraud efforts are mainly focused on prevention, as we have a legislative and methodological framework in place, including the implementation of effective control systems, and staff are trained to recognise fraudulent behaviour and risk situations. This approach is considered the most effective, as strengthening preventive measures directly contributes to reducing the incidence of irregularities and fraud.

Q.1.4 Which part of the Anti-Fraud Cycle do your Anti-Fraud Efforts target most?

Response	Frequency	Percentage	Member States
Recovery	12	44.4%	BE, BG, DK, ES, FR, HU, IE, LV, NL, PL, SE, SK
Investigation	11	40.7%	CY, CZ, DE, EE, EL, FI, HR, LU, PT, RO, SI
Prevention	3	11.1%	AT, IT, MT
Detection	1	3.7%	LT

Q.1.5 Please explain your reasons for this choice

Member State	Response
AT	ALL parts are covered. NOTE: It is therefore not possible to specify, in reply to Q.1.4, which part is 'targeted most'.
	Which part of the Anti-Fraud Cycle do your Anti-Fraud Efforts target least?
BE	BE AFCOS: There is an increased focus on the recovery of funds throughout the Belgian network. With budgets under pressure amid all partners recovery is an essential part of an effective system. Nonetheless compared to the efforts made in all parts of the anti-fraud cycle we noticed the efforts concerning recovery are not yet at the level of the other anti-fraud stages. PSW (Public Service of Wallonia) ERDF Wallonia: The PSW has invested heavily in prevention and detection and already has a solid system for recovery available to it. Efforts in 2026 will focus on the investigation cycle. The PSW aims to harmonise procedures for treating internal and external irregularities and to contribute to improving relations with judicial authorities. The correction and prosecution phases take place ex post but are nonetheless important to the PSW. The application of visible sanctions serves as a deterrent. FPS Finances (Customs disputes): Other departments' mandates are to carry out prevention, detection and investigations. ERDF and RRF Brussels Capital Region: The greatest focus is on prevention and detection, meaning that the focus on investigation and recovery is lesser in comparison. Nevertheless, measures have been taken to investigate identified irregularities and potential cases of fraud, and where necessary, to address these (for example checking and analysing expenditure, carrying out supervisory missions, etc.).
BG	The overly broad regulatory scope of securities/collateral makes it difficult for the managing authorities to exercise their recovery rights when imposing financial corrections. The investigation of fraud falls within the competence of the national law enforcement authorities. There is a significant delay in the investigation of crimes by law enforcement agencies
CY	The investigation phase is comparatively less directly targeted by the NAFS because the Strategy's principal function is to strengthen the horizontal anti-fraud system, while investigative and prosecutorial powers remain with specialised competent authorities under their respective legal mandates. The NAFS can add most value before and around the investigation phase: by improving prevention, risk assessment, detection, reporting channels, referral mechanisms, information exchange and coordination. Once a suspected fraud case reaches the investigation stage, action depends on the applicable administrative, criminal or EU-level procedures and on the mandates of bodies such as national investigative authorities, the Law Office of the Republic, EPPO and OLAF. Accordingly, the Strategy does not seek to duplicate or interfere with these functions. Instead, it supports them indirectly by strengthening investigative capacity, clarifying referral and communication protocols, improving the quality of information transmitted to competent authorities and promoting more consistent inter-agency cooperation.
CZ	Investigations in the legal sense are conducted by the law enforcement authorities rather than bodies of the implementation system. In a more general sense, the latter bodies must, as part of their control activities, find out as much information as possible about the irregularity detected and reach their own conclusion so that they can pass the matter to other competent authorities. Investigations are usually carried out at the first stage. They are then passed on to the authorities responsible, such as the law enforcement authorities.

Member State	Response
	Investigations of suspected fraud cases are carried out by the law enforcement authorities and other competent bodies, and not by the Ministry's control department.
	The Rhineland-Palatinate ERDF managing authority: Under administrative proceedings, the focus is on prevention and detection, given that investigation is primarily the task of the law enforcement authorities. The NRW ERDF managing authority: Confirmed fraud leads to automatic recovery. There are well-established national procedures in this regard. The Saxony-Anhalt ESF managing authority: In Germany, the law enforcement authorities are responsible for investigation. The Lower Saxony ERDF managing authority: By applying the reimbursement procedure and carrying out thorough checks, possible attempts at fraud can be detected even before the funds are paid out. The ESF Plus Federal Programme, led by the Federal Ministry of Labour and Social Affairs (BMAS): The focus is on prevention and detection for preventive and efficiency-related reasons. Consequently, the number of cases of fraud or suspected fraud can be reduced from the outset in a pre-emptive manner, meaning there is naturally less need for investigation and recovery. The Schleswig-Holstein ERDF managing authority: There have been no recent cases of ERDF-related fraud in Schleswig-Holstein. Therefore, it has not been necessary to carry out any investigations.
DE	The Bremen ERDF managing authority: Investigating possible attempts at fraud falls within the remit of the public prosecutor's office or its delegated bodies. The task of the core administration is to identify possible intentions of fraud, to step up the administrative checks in case of suspicion, and, if the suspicion is confirmed, to report it to the managing authority and the public prosecutor's office. The AMIF managing authority: The recovery of EU funds usually takes the form of reductions in grants. These are often the result of irregularities being detected and investigated and not the stated aim. The aim is to ensure that the grant system operates in a reliable and transparent manner and is as free as possible from irregularities, and that irregularities are investigated and corrected. If and insofar as the recovery of funds is warranted, the process is initiated as quickly as possible to prevent losses for the EU budget. The Hessen ERDF managing authority: statutory division of responsibilities at national level: investigations are carried out (after a criminal complaint has been filed) by the competent public prosecutor's office/the European Public Prosecutor's Office. The Thuringia ERDF managing authority: Prevention is key. Effective prevention allows the intermediate body to better exercise its responsibilities. The implementing bodies are also in a position to detect irregularities at an early stage and take the necessary measures. The aim is to take an early decision on reportable cases so that OLAF can be involved as soon as possible. The Baden-Württemberg ERDF managing authority:

Member State	Response
	As soon as there is a suspicion of fraud, the case is referred to the competent law enforcement authorities, which are responsible for investigating the suspected fraud further. Investigations are also carried out as part of administrative-law proceedings in order to protect the financial interests of the EU budget. The Brandenburg ERDF managing authority: As effective prevention is the first priority, in many cases there is no need for recovery, as no payment has been made at all. While the recovery of EU funds following a fraud case is an important mechanism, preventive measures should be prioritised in the fight against fraud. This not only protects the EU budget from losses in the long term, but also ensures that EU funds are used more efficiently and responsibly, in the best interests of citizens and the EU as a whole.
DK	In general, we experience a low degree of fraud or suspected fraud. Combined with a strong system for detection, recovery is rarely a relevant course of action. When relevant, we don't experience any difficulties in recovering funds.
EE	While our anti-fraud efforts span the entire Anti-Fraud Cycle, the phase in which we are least directly involved is the criminal investigation stage. This is not because criminal proceedings are any less important—on the contrary, they are essential—but the EPPO Regulation limits the active role AFCOS units can take in EPPO-led investigations, and AFCOS does not typically represent cases in that context. Cooperation with prosecutors remains smooth, constructive, and highly valued. In administrative proceedings, however, we are fully engaged in detection, clarification, and recovery activities. Since the operational focus of the grants implementation system is on prevention—particularly through risk assessment and ex-ante controls—many issues are addressed before they escalate. When irregularities do occur, we handle them comprehensively through administrative detection and recovery mechanisms.
EL	Special Service for Institutional Support and Information Systems (EYTHYPS): Management and control system (MCS) procedures cover the detection and documentation of suspected fraud. Further investigation and the treatment of cases under criminal or administrative law do not fall within the jurisdiction of the MCS authorities but are carried out by the competent national bodies and judicial authorities of the Hellenic Republic, in accordance with the current institutional framework. Recovery and Resilience Facility Special Coordination Service (EYSTA): EYSTA has no powers to investigate irregularities indicating fraud. Investigative powers have been conferred to and are exercised at the national level by specific bodies and services.
ES	The implementation of robust controls and preventive measures and effective early detection mechanisms significantly reduces the likelihood of fraud materialising or having a significant financial impact. It is therefore the effectiveness of the prevention and detection phases that would justify devoting less effort to the later phases of the anti-fraud cycle. For the managing authorities, investigation and recovery are reactive and subsidiary in nature and only come into play in specific cases, whereas prevention and detection are ongoing, cross-cutting activities integrated into all management procedures. In the case of investigation, this is normally carried out by specialised entities, while the role of the managing authority and intermediate bodies focuses on communication, coordination and the application of any corrective measures that may arise (withdrawal of expenditure, refunds). In the case of recovery, the lesser efforts devoted to it can be justified because, at national level, in accordance with current legislation, reimbursement procedures are fully established, systematised and operational, and their application constitutes a direct legal

Member State	Response
	obligation that does not require further development to ensure their effectiveness in the field of European funds.
FI	The focus of anti-fraud efforts is on a well-functioning and effective administrative and control system that prevents fraud.
FR	We experienced technical difficulties with the introduction of effective tools to achieve this objective.
	Note: Considering that the question should be "Which part of the Anti-Fraud Cycle do your Anti-Fraud Efforts target least?" these are the answers:
	Contribution from the Ministry of Agriculture, Forestry and Fisheries (Paying Agency for Agriculture, Fisheries and Rural Development): In the case when the irregularity contains ascertaining elements related to suspicion(s) of fraud against EU financial interests, Paying Agency send the report/document as well as relevant documentation to the EPPO in order to analyse what measures should be taken in accordance with the legal provisions.
HR	Contribution from the Ministry of Labour, Pension System, Family and Social Policy: This is part of the anti-fraud cycle that is covered by other institutions specialised in frauds investigation, such as EPPO and the State Attorney's office. Contribution from the Ministry of Regional Development and EU funds: Our anti-fraud efforts do not target any part of the Anti-Fraud Cycle least. All four elements – prevention, detection, investigation, and recovery – are addressed in a balanced and integrated manner, as they are equally important for ensuring effective protection of the EU's financial interests. Bodies within the management and control system for the use of ESI Funds are responsible for implementing measures across the entire cycle, from preventing and detecting irregularities and suspected fraud to ensuring appropriate follow-up, reporting and recovery of unduly spent funds. Contribution from the Ministry of Finance, Customs Administration: We do not conduct investigations, that is the responsibility of other bodies. We cooperate in certain stages of the procedure if necessary.
HU	The National Anti-Fraud and Anti-Corruption Strategy (NAFS) for European Union funds was adopted as a national institutional strategy in Hungary, in order to avoid redundancy with the policy-level National Anti-Corruption Strategy (NACS). Institutions set up to perform tasks related to EU funds have limited means to recover assets in the absence of cooperation from the beneficiary or other relevant stakeholders (the tax administration and judicial bodies can act in the case of asset recovery).
IE	The majority of cases that are identified through investigation processes do not transpire to be proven cases of fraud, which can be credited to the prevention and detection systems currently in place. In addition, as expenditure is incurred via the Exchequer Vote process initially, any instances of fraud/suspected fraud fall within the anti-fraud policies of the government department and are excluded from expenditure claims. Therefore, recoveries do not occur regularly due to this.
IT	All stages are taken into consideration as part of anti-fraud efforts.
LT	We do a lot of analytical work to identify the cause of financial fraud.

Member State	Response
LU	Which part of the Anti-Fraud Cycle do your Anti-Fraud Efforts target least? The investigation would be the responsibility of the national jurisdictions and/or EPPO, in case we would detect a fraud or suspicion of fraud.
LV	Fraud investigation becomes the second most important activity because it ensures accountability, closes control gaps, and deter future fraud, as well as protects organisational integrity and public trust.
MT	Same as above. Kindly vide Malta's provided in Questions 1.3 and 1.6.
NL	Again, different parties approach the fight against fraud from slightly different angles. For example, the managing authorities (expenditure) focus least on recovery and Customs (revenue) focus least on prevention.
PL	Each stage of the anti-fraud cycle is the responsibility of the competent institutions or services in the area concerned. Within their remit they take appropriate measures to combat fraud in accordance with treaty obligations, EU regulations and national law. Where appropriate they cooperate and exchange information with each other. Recovery might constitute a relatively weak part of the cycle given how long recovery proceedings last, due, for example, to appeals and court proceedings.
PT	Our answer to the previous question (Q.1.4) concerns a part of the anti-fraud cycle to which relatively little attention is currently devoted. The anti-fraud coordination service (AFCOS) and the bodies involved in handling and monitoring European funds have no mandate to investigate cases with signs of fraud. However, they do have reporting channels and encourage the Ministério Público (public prosecutor) to become involved where potential cases of fraud have been detected. It then falls to the bodies in question to conduct the investigations. Protocols have been drawn up for coordination between the bodies responsible for handling and monitoring European funds and judicial bodies, including a cooperation protocol between the inspectorate-general of finances (IGF) and the Procuradoria-Geral da República (office of the prosecutor-general), which was adopted on 7 April 2005 at the IGF's annual general meeting.
RO	Following consultation with the bodies listed in the reply to question 5.1, it became apparent that the answers to this question vary and are specific to the activities of each body and cover all parts of the anti-fraud cycle. Their detailed responses are presented below. National Agency for Public Procurement: Investigating fraud falls within the remit of criminal investigation authorities and other authorised bodies, rather than the National Public Procurement Agency. Ministry of Energy: The limited number of staff involved in investigating and resolving suspected irregularities makes the prevention and detection stages difficult to implement. To remedy these deficiencies, platforms and algorithms could be created to prevent the emergence of suspicions of irregularities. Ministry of Investments and European Projects: Fraud investigations do not fall within the Managing Authority's remit. North-East Regional Development Agency: Investigations are conducted by institutions authorised by law. Any suspicions of fraud identified within our organisation are referred for investigation to the Romanian Anti-Fraud Directorate, the European Public Prosecutor's Office and/or the National Anti-Corruption

Member State	Response
	Department. West Regional Development Agency (recovery): Given the current stage of implementation of the 2021-2027 West Regional Programme, the number of suspected irregularities or cases of fraud is low. South-West Oltenia Regional Development Agency: Criminal investigations fall within the remit of other specialised national authorities. The Managing Authority's role is limited to prevention, detection, reporting and administrative recovery, in compliance with the division of responsibilities under national and European legislation. North-West Regional Development Agency: There were no suspected cases of fraud in 2024.
SE	Recovery is the least resource-intensive area. Investigating and proving fraud is a matter for the judicial system.
SI	The MKRR explains: For this part, most competences lie with other authorities. To that end, as the MA for ESI funds, the MKRR has stepped up its cooperation over the past year with the European Delegated Prosecutor's office in Slovenia and the criminal police, with a focus on investigations. This measure is also described in the questionnaire on the implementation of Article 325 by the Member States (2025 PIF Report).
SK	Recovery is one of the key activities of the MA/IB, as they are responsible for timely reporting and updating irregularities and for taking all steps to recover ineligible expenditure in a timely manner. Despite the measures in place (legal and methodological framework, controls, audits carried out), there are still differences between the amounts recommended for recovery and the amounts actually recovered from the entity that caused the irregularity. At the same time, the recovery process can be legally and administratively complex.

Q.1.6 How do you measure the effectiveness of your Anti-Fraud system?

Member State	Response
AT	BMLUK: All cases of suspected fraud reported by the paying agency are studied by the certification body. The evolution in cases is monitored. The Finanzprokuratur [Lawyer and legal advisor of the Republic of Austria] is called in in cases of doubt. BMASGPK: In view of the very small number of ESF fraud cases in Austria, the system can be considered effective and efficient.
BE	Belgian AFCOS: By the level by which the secretariat of the Belgian AFCOS has been contacted for advice and input on the matter. Due to its decentralised structure other effort to measure effectiveness are taken by the respective partners.

Member State	Response
	PSW ERDF Wallonia: At the PSW, we have put in place a self-assessment tool for fraud risks, which functional administrations in charge of European funds are required to fill in and update once a year. A form for the self-assessment of cross-cutting fraud risks, to be filled in by each department, is also in the process of being drawn up. Recommendations in the audits carried out by the CAIF (Cellule Audit de l'Inspection des Finances) and the European Commission are also opportunities to challenge our system and to improve it on a regular basis. The PSW has also set up some working groups, 'Mira Anti-Fraud' and 'OLAF', which allow for brainstorming the various current measures and improving them, or for implementing new ones. ERDF and RRF Brussels Capital Region: Through the internal collecting of data and information relating to detected irregularities and (potential) instances of fraud. EUROPA WSE (ESF VL): We do not currently measure the effectiveness of our Anti-Fraud system.
BG	The system is the National Strategy for the Prevention and Combating of Irregularities and Fraud affecting the Financial Interests of the European Union for the Period 2021-2027. A large part of the employees involved in the fight against fraud use the Arachne tool. There is institutional coordination between the various units involved in the fight against fraud. The effectiveness of the anti-fraud system within some of the MA is measured by the fraud risk self-assessment. If necessary, additional measures are planned and implemented
CY	Currently the effectiveness is not formally assessed. The annual assessment of the anti-fraud efforts is one of the KPIs of the action plan for the NAFS which has been finalised.
	By the number of detected cases of suspected criminal activity and the success rate in criminal proceedings. By the number of fraud cases detected.
CZ	We observe the number and value of fraud cases detected, the number of checks and the regular evaluation of fraud risks. The effectiveness of the anti-fraud system is assessed not as a whole but based on the results of controls and investigations: mainly by the number and nature of irregularities identified and their subsequent handover to the bodies concerned for follow-up. By the ratio of total projects to identified cases.
DE	The Rhineland-Palatinate ERDF managing authority: On the basis of the level of detail and quality of the following: reports submitted by the intermediate bodies, on-the-spot verifications, checks carried out by the audit authority, and system checks carried out by the managing authority. Any shortcomings in the fraud prevention system can be identified through this. The Saxony-Anhalt ESF managing authority: The number of suspicious cases detected by the management and control system and the audit authority. The ESF Plus Federal Programme, led by the Federal Ministry of Labour and Social Affairs (BMAS): A regular self-assessment is carried out of the managing authority's strategic approach to preventing and combating fraud and corruption. This self-assessment incorporates all the

Member State	Response
	available information on combating fraud and exchanges between the relevant stakeholders, for example on ongoing cases of fraud and suspected fraud involving the ESF and the main identified risk areas, so as to enable emerging risks and fraud trends to be investigated and addressed in a timely manner. The Bremen ERDF managing authority: The number of possible fraud attempts reported (no reports thus far); the results of audits of operations carried out by the audit authority; verification of the effectiveness of control mechanisms using the self-assessment tool. The AMIF managing authority: The framework is established on the basis of rules in our funding guidelines and funding manual, as well as the internal guidelines on handling irregularities. Alongside the management and control system, (fraud) risk management and risk analysis, a control framework has been established. Moreover, the quality assurance and reporting channels, the audits of operations carried out by the audit authority and the self-declarations requested from applicants facilitate monitoring and serve to prevent and combat fraud. Detected cases of irregularities are also collected, counted and analysed centrally. The reasons for the irregularities, the results of the investigations, and the follow-up measures and their effectiveness are analysed. The control mechanisms are updated on an ad hoc or regular basis. The control strategy was revised in 2025. As a result, more thorough checks are carried out on evidence of use of funds. The number of cases and adjustments make it possible to measure the effectiveness of the fraud prevention system quantitatively and qualitatively. The Hessen ERDF managing authority: Regular programme-specific fraud risk assessment in line with the presentation of a risk assessment tool by the Commission (see guidance document). Depending on any residual risks identified, supplementary anti-fraud measures are implemented in the management and control system. The Thuringia ERDF managing authority: Effectiveness is not specifically measured. Reports on suspicious cases and audits of operations are used to draw conclusions about the fraud prevention system. In the case of frequent reports or prominent cases involving operations, appropriate adjustments are made to the fraud prevention system. The Baden-Württemberg managing authority: On the basis of continuously updated fraud statistics, which now cover three funding periods and show a very low number of cases. The Brandenburg ERDF managing authority: Statistics and a list of suspected fraud cases from cross-checks with all operations in the funding period. Very low number of confirmed cases of fraud, given the number of applications for which no payment is made once fraud is suspected and also the number of cases of suspected fraud reported to the competent investigating authorities which actually result in a conviction entailing a fine and/or imprisonment.
DK	Danish Business Authority: We don't have a formal system in place to measure the effectiveness of our anti-fraud efforts. It is our experience that we rarely get a case of fraud even though projects are continuously monitored by several different parties. This is in part because of the general low amount of fraud in our country but also suggests that our preventive and control measures are working effectively. Danish Agricultural and Fisheries Agency: Varies. Regarding detection, operationability and usability of, e.g. "Red flags" for case

Member State	Response
	workers is essential. Regarding recovery, the success-rate in recovering irregular or wrongful amounts is used as measure.
	We measure the effectiveness of our Anti-Fraud system through a combination of quantitative indicators and qualitative assessments across all stages of the Anti-Fraud Cycle. Key elements include: Prevention indicators: - quality and depth of risk assessments - the proportion of applications flagged or adjusted based on preventive controls - reduction in the number of cases escalating into detection or investigation phases Detection and administrative investigation metrics: - number and type of irregularities identified in administrative checks - timeliness and accuracy of case clarification - patterns or recurring issues that signal system-level vulnerabilities
EE	Recovery performance: - amounts recovered through administrative procedures - recovery rate relative to identified financial impact - time required to complete recovery processes System-level impact: - overall decrease in downstream cases requiring resource-intensive investigation or recovery - feedback from internal and external audits - alignment with regulatory requirements and cooperation frameworks Our overarching goal is to ensure that strong preventive controls reduce the need for later-stage interventions, while maintaining the capacity to detect, clarify, and recover losses effectively when issues do arise.
	Special Service for Institutional Support and Information Systems (EYTHYPS): The effectiveness of the anti-fraud system is measured using a combination of quantitative and qualitative data, such as the number of detected suspicions of fraud, results from audits and verifications, and the findings of the Financial Audit Committee (EDEL) and EU audit bodies.
EL	Recovery and Resilience Facility Special Coordination Service (EYSTA): In accordance with the Manual of MCS Procedures for the National Recovery and Resilience Plan, EYSTA carries out a yearly assessment of fraud risks and of the effectiveness of the preventive measures that have been incorporated into the applicable MCS. The assessment is based on the results of the planned audits carried out both by EYSTA itself and by other competent national and European bodies. If new risks are detected, EYSTA takes initiatives to plan new measures and incorporate them into the MCS to mitigate these risks, and then amend the Fraud Risk Assessment Methodology, so that the estimate of the overall risk remains at acceptable levels.
	The responses from the various authorities consulted include the following measures or mechanisms applied to assess their effectiveness:
ES	- The effectiveness of the anti-fraud system is measured through a set of qualitative and quantitative indicators focused mainly on the prevention and detection phases, which make it possible to assess the system's ability to minimise the risk of fraud and detect possible irregularities at an early stage. In particular, the degree of implementation and compliance with preventive controls, the results of periodic controls and verifications, and the absence or low incidence of significant irregularities are considered essential. Similarly,

Member State	Response
	it is considered necessary to analyse the number, type and recurrence of alerts or indications detected, as well as the time taken to identify and deal with them, and the evolution of the residual risk of fraud, assessed through periodic risk analyses and self-assessments of the anti-fraud system. - The effectiveness of the anti-fraud system is measured primarily through a risk-based continuous improvement approach, supported by these key elements: - Periodic risk self-assessment exercises (matrices): these are carried out periodically and allow for a comparison of inherent risk vs. residual risk, validating whether the controls implemented reduce it to acceptable levels. The results are reviewed, distributed internally and, if necessary, lead to action plans and additional controls. - Follow-up of corrective actions: supervision of the implementation of measures derived from the self-assessment and evaluation of their impact, adjusting controls when new risks or inefficiencies are detected. - Results of controls and verifications (administrative and on-site), together with the use of red flags, which make it possible to check in practice whether the detection mechanisms are working and whether the net risk is decreasing. - Analysis of irregularities and feedback: the recording and monitoring of detected cases, as well as the withdrawal of irregular expenditure and refunds, serve to identify weaknesses in the system and strengthen internal procedures. - Collection of data from the anti-fraud system, such as the number of complaints, the number and identification of offending companies, etc., with a system of indicators of the effectiveness of the anti-fraud system (ratios of complaints per channel, infringements by type of project, infringements reported to the competent authorities) currently being implemented. An indicator has been implemented, number of complaints in relation to the number of cases handled each year, which has remained at levels considered minimal, both in relation to historical data and in comparison with other similar organisations.
FI	Anti-fraud procedures are assessed on the basis of fraud risks, the effectiveness of the measures in place, the strength of the control system, the level of training and the findings of the audit and certifying authority. The assessment is based on the European Commission's detailed guidance, which will be developed continuously and systematically.
FR	Through audits conducted by the CCCOP (Commission for the Certification of the Accounts of Paying Agencies) and the AnAFé (National Authority for the Audit of European Funds)
HR	Contribution from the Ministry of Agriculture, Forestry and Fisheries (Paying Agency for Agriculture, Fisheries and Rural Development): Undertaking fraud risk assessments. Contribution from the Ministry of Agriculture, Forestry and Fisheries, Directorate of Fisheries: Mostly, the measurement is based on the number of irregularities and suspicion of fraud/fraud detected whereas the less cases are detected or more cases are prevented, the Anti-Fraud system is more effective. Contribution from the Ministry of Regional Development and EU funds: Our Anti-Fraud system is considered effective, as it ensures the prevention, detection and correction of irregular or fraudulent behaviour throughout the implementation of ESI Funds. We measure its effectiveness through the results of preventive, detective and corrective measures within the management and control system, including the timely detection and

Member State	Response
	reporting of irregularities, the follow-up of suspected fraud cases, and the application of financial corrections and recovery of unduly paid amounts. The system's effectiveness is further assessed through audit findings, management verifications, risk assessments, and continuous improvement activities such as training and awareness-raising for relevant bodies and beneficiaries.
HU	The effectiveness of the strategy is monitored through the implementation status of the measures set.
IE	This is measured by the small number of proven case and relatively small amounts of funding involved in proven fraud cases following investigation at each year end
IT	The effectiveness of the anti-fraud system is measured by the ability to detect cases of irregularities and/or fraud as soon as possible in order to avoid the disbursement of funds and/or to launch the procedures for the recovery of funds already paid in a timely manner. Other elements taken into account are the degree of coordination and cooperation between the national and European authorities involved, as well as the effective implementation of the preventive and corrective measures taken. Specifically, the effectiveness of anti-fraud measures are assessed mainly through: (i) periodic risk self-assessment, which may be followed by corrective action; (ii) results of the first-level management checks; (iii) results of the audit of operations and system audit.
LT	We are positive, because the number of reports from Agencies is decreasing.
LU	We regularly conduct a risk analysis that includes not only the identification of potential risks but also a review of recent irregularities. Because this number fluctuates over time, it provides us with a clear indication of whether the measures we implement are effective. Given that the number of fraud cases within our fund remains consistently very low, we can confirm the overall effectiveness of the systems and controls we have in place.
LV	All EU funds institutions have an internal control system for combating fraud, which is periodically improved and operates effectively. Preventive and control measures have been introduced for the timely identification of fraud risks, and fraud cases are assessed.
MT	Prevention, detection and recovery of irregularities and suspected cases of fraud are dealt with by the Managing Authorities (Planning and Priorities Coordination Division and Funds and Programmes Division) and Paying Agency (Agriculture and Rural Paying Agency) of European Union (EU) funds. Detection is also managed by the Audit Authority and Certifying Body of EU funds. Cases of suspected fraud are forwarded and dealt with by the Financial Investigations Directorate (FID) within the Internal Audit and Investigations Department. In addition, FID, in its role as the Maltese AFCOS, also holds a quarterly Irregularity Reporting Sub-Group meeting between the above-mentioned national authorities. The meeting is held to ensure correct and complete reporting of irregularities and suspected cases of fraud by the Maltese AFCOS in the Irregularity Management System (IMS).
NL	Here too, there are differences. For example, Customs (revenue) uses sampling. For expenditure, a fraud risk cycle is applied in which the accuracy of the risk analyses is checked retrospectively. There is also constant monitoring.
PL	The indicators considered when measuring the effectiveness of the anti-fraud system in cohesion policy include: 1. The existence of procedures, adopted in each programme, covering areas such as the fight against irregularities and fraud. 2. Regular fraud risk assessments and application of the results of such analysis in the preparation of annual control plans. 3. The number of views of the educational materials on YouTube concerning the fight

Member State	Response
	against fraud, including conflicts of interest. 4. The available channels for reporting irregularities and red flags. 5. The use of data analysis tools. 6. The assessment results included in reports on audits of the management and control system carried out by the Audit Authority. The indicators considered when measuring the effectiveness of the anti-fraud system in agricultural policy include: 1. The results of analyses, verifications and comparison of available data. 2. The results of the quarterly monitoring of cases where fraud is suspected. 3. The results of the quarterly monitoring of cases referred to the law enforcement authorities. 4. The results of the quarterly monitoring of cases where fraud has been confirmed.
PT	The NAFS sets measurable indicators and targets enabling us to ascertain the implementation level of each of its measures. National Agency for Public Procurement: Through continuous monitoring and control activities, as set out in the operational procedures. Paying and Intervention Agency for Agriculture: By correlating prevention with detection and recovery, we have achieved our objectives. Ministry of Energy: This was achieved by: ensuring the effectiveness of the procedural system through user compliance; consulting dedicated platforms such as Arachne, ONRC, REGAS and www.dubla-finantare.ro; and concluding partnerships with other public institutions to prevent double funding. Warning systems should be set up within the platforms used to identify businesses applying for European funds that may present potential eligibility-related vulnerabilities. Ministry of Investments and European Projects: The number of fraud notifications confirmed as such.
RO	North-East Regional Development Agency: Following the checks carried out during the audit visits, the conclusion on the effective functioning of the management and control system at the level of key requirement 7 is as follows: 'The system works. Some improvements are needed (category 2)'. In addition, the internal fraud risk assessment found that the consistent application of preventive measures and internal checks by the Managing Authority has significantly strengthened the anti-fraud control system and reduced the risk of fraud in the use of funds. However, ongoing monitoring is necessary to ensure that anti-fraud measures laid down in specific operational procedures remain effective and are adapted to emerging threats. West Regional Development Agency: The management and control system is verified by the Audit Authority within the Romanian Court of Auditors. The management and control system of the Managing Authority for the West Regional Programme currently falls under category 2: 'The system works. Some improvements are needed'. South-West Oltenia Regional Development Agency: We assess effectiveness by monitoring the results of management verifications, the number and type of irregularities identified, the financial corrections applied, and the amounts recovered; by complying with reporting deadlines; and by constantly improving the internal procedures and the risk analysis tools used.

Member State	Response
	North-West Regional Development Agency: As a result of the anti-fraud measures adopted by the North-West Regional Development Agency and the implementation of activities to prevent and mitigate fraud risks, the system adopted is highly effective.
SE	We monitor the number of OLAF notifications and recoveries.
SI	Effective.
SK	Effectiveness is assessed based on closure rates, time to recovery, and implementation of corrective actions following reported irregularities.

Q.1.7 (IMS users) How do you ensure adequate knowledge of existing staff?

Response	Frequency	Percentage	Member States
OLAF/Commission issued materials	22	81.5%	AT, BE, BG, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LU, LV, MT, NL, PL, PT, RO, SI, SK
Regular training sessions	20	74.1%	AT, BE, BG, CZ, DE, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, NL, PL, RO, SE, SI
Liaison officers/ Trainers in contact with OLAF	18	66.7%	AT, BE, BG, CY, CZ, DE, ES, FI, FR, HR, HU, IE, MT, PL, PT, RO, SI, SK
National IMS Guidance/Guidebooks	17	63.0%	BE, BG, CZ, DE, DK, EL, ES, FR, HR, HU, IE, IT, LV, PL, RO, SI, SK
Other (please specify)	11	40.7%	AT, BE, CZ, DE, EE, EL, HU, IE, LV, NL, SK

Following Q1.7, please specify "Other".

Member State	Response
AT	Training as required.
BE	ERDF and RRF Brussels Capital Region: Internal documents and some training sessions and/or workshops from time to time.
CZ	Communication between reporting entities/sharing of good practice.
DE	The Federal Office for Agriculture and Food (BLE): Internal material. The Thuringia ERDF managing authority: Relevant training material is provided by the European Commission. Staff use this material for professional development and to keep their knowledge up to date in relation to irregularities.
EE	We ensure adequate knowledge of our IMS users through a combination of experience-based competence and structured support mechanisms. In Estonia, the number of IMS users is relatively small, as most operational data is maintained in national databases and only uploaded to IMS when required. As a result, our IMS users are long-standing staff members with substantial practical experience in both the system and the underlying administrative processes. Whenever questions or technical issues arise, users receive direct guidance from the Country Officer, who liaises with OLAF colleagues when necessary. This ensures that our users remain up to date with system requirements, procedural changes, and best practices, even though the user base is limited. The combination of experienced staff and reliable support channels allows us to maintain a consistently high level of IMS-related knowledge.
EL	Through the anti-fraud network composed of staff from the Managing Authorities of the Partnership Agreement for Regional Development (ESPA) programmes.
HU	AFCOS organises regular (quarterly) irregularity-reporting working group meetings for reporting bodies to discuss current policy issues.
IE	IMS training took place in Dublin in October 2025, with representatives from each reporting authority in attendance in-person and online. The reporting structure has been restructured in 2025 and efforts to solidify this will continue in 2026. Country Officers have been put in place. An AFCOS Network handbook had been in production. This is an initiative led by AFCOS, in consultation with all reporting authorities and OLAF. It is due for adoption imminently.
LV	Additional information posted in IMS system (library) regarding the completion of individual fields, as well as emails from the IMS team, which sometimes provide recommendations/instructions for entering information into the system or completing specific fields.
NL	Instructions are drawn up for staff dealing with registration in IMS. The team has also been the same for years. If new staff are assigned this task in the future, they will receive training, for which the OLAF manuals will be a good guide.
SK	Guidance for IMS users within the AFCOS network is also provided through individual consultations in particular when dealing with specific cases and technical or

Member State	Response
	methodological issues related to the reporting of irregularities, as well as within the Irregularities Working Group established under the Steering Committee for the Protection of the European Union's Financial Interests, where recurring problems, the most common errors in reporting and proposed measures to improve the quality and completeness of data are discussed. AFCOS network partners have the opportunity to discuss and present proposals and jointly resolve issues related to improving the protection of financial interests.

Q.1.8 (IMS users) How is new staff trained on existing reporting and coordination procedures related to IMS?

Response	Frequency	Percentage	Member States
Specification of responsibilities ensuring clear attribution of tasks	19	70.4%	AT, BG, CZ, DE, ES, FR, HR, HU, IE, LT, LU, LV, MT, NL, PL, PT, RO, SE, SI
Coordination at National level	17	63.0%	AT, BG, CY, CZ, DE, EE, ES, HR, HU, IE, IT, LU, PL, PT, RO, SE, SI
Extensive written documentation of necessary tasks	16	59.3%	BG, CZ, DE, DK, ES, FI, HR, IE, LU, LV, NL, PT, RO, SE, SI, SK
National IMS Guidance/Guidebooks	16	59.3%	BE, BG, CZ, DE, DK, EL, ES, HR, HU, IE, IT, LU, LV, PL, SI, SK
A Grace Period involving the new and old hire	7	25.9%	BE, DE, HR, IE, LU, SI, SK
Coordination at Regional level	6	22.2%	AT, DE, ES, IE, LT, PL
Transfer of the case responsibility ownership	5	18.5%	BE, DK, HR, IE, LU
Coordination with other Member States	4	14.8%	AT, CZ, HR, IE

Response	Frequency	Percentage	Member States
Other (please specify)	9	33.3%	BE, CZ, DE, FI, HU, IE, MT, PL, SK

Following Q.1.8, please specify "Other".

Member State	Response
BE	ESF VL EUROPA WSE: As we only have one person responsible for IMS, there is no training readily available at this moment. ERDF & RRF Brussels-Capital Region: Internal information transfer and documentation of the persons with specific responsibilities and knowledge regarding irregularities and fraud.
CZ	Pooling of good practice between colleagues.
DE	The ESF Plus Federal Programme, led by the Federal Ministry of Labour and Social Affairs (BMAS): As part of the induction for new staff, information is provided about the reporting procedure. The material issued by OLAF and the national IMS guidelines/guidance documents are made available in a central information database. The AMIF managing authority: Comprehensive training, awareness-raising and induction of new staff. The AFCOS, the Federal Ministry of Finance: Regular workshops for IMS users in order to present current developments and issues in relation to recording irregularities in the IMS, provide solutions and improve data quality.
FI	In-person training, limited number of users.
HU	The AFCOS senior IMS expert provides practical IMS training for all new IMS users when IMS privileges are made available.
IE	Work in this space is ongoing, ensuring staff and namely country officers are trained up. Support from OLAF has been of huge benefit across the Irish system.
MT	New staff is trained by IMS managers, OLAF IMS training and also through OLAF/Commission issued materials.
PL	- Training courses for new staff; - Mentoring during the first few quarters of work; - Institutions' in-house training material on the rules for making reports in IMS, covering the use for that purpose of data from institutions' own information systems.
SK	Guidance for IMS users within the AFCOS network is also provided through individual consultations in particular when dealing with specific cases and technical or methodological issues related to the reporting of irregularities, as well as within the Irregularities Working Group established under the Steering Committee for the Protection of the European Union's Financial Interests, where recurring problems, the most common errors in reporting and proposed measures to improve the quality and completeness of

Member State	Response
	data are discussed. AFCOS network partners have the opportunity to discuss and present proposals and jointly resolve issues related to improving the protection of financial interests.

RECOMMENDATION 2 – ESTABLISHING MORE EFFECTIVE COMMUNICATION CHANNELS

Better coordination between national authorities, OLAF and the EPPO is also necessary to ensure that cases investigated by EU bodies are duly reported at the earliest possible moment in compliance with the relevant EU sectoral legislation. National authorities must correctly identify and address existing loopholes in the information flow in relation to suspected fraud, the moment they are first reported, and even more so, when following-up on them both in judicial and administrative proceedings at national level. The Commission is committed to further developing and providing the necessary guidelines, IT tools and support. The Commission will also

Q.2.1 (AFCOS) What systems/practices do you have in place to ensure uninhibited information flow between judicial and reporting authorities?

Member State	Response
AT	E-Mails.
	Belgian AFCOS: As previously stated, the decentralised structure in Belgium has as a result that communication between reporting and judicial authorities does not necessarily run through the BE AFCOS Secretariat. However, we are in close contact with the Belgian magistrates of the EPPO and invite them during the AFCOS sessions to inform all partners of the current situation. The Secretariat is also capable of transferring the necessary information to the judicial authorities by writing an investigation report under art 29 Belgian Code of Criminal Procedure.
BE	PSW ERDF Wallonia: (PSW) At the Walloon regional level, a workflow already provides for procedures laid down in regional legislation to pass on fraud cases to the Public Prosecutor's Office (Article 20 of the Decree of 28 February 2019 on the monitoring of laws and regulations on economic policy, employment and scientific research policy, and also the introduction of administrative fines for breaches of these laws and regulations). The Public Prosecutor's Office procedure for sending information between the Belgian Public Prosecutor's Office (PPO) and the European PPO allows for a rapid transfer of cases (Circular No 03/2022 of the College of Principal Public Prosecutors). A procedure for addressing and correcting fraud is being drawn up at PSW level.
BG	Reporting authorities request regular reports from judicial authorities
CY	We are in the process of acquiring a whistleblowing platform that will be used as a case management tool.
CZ	Established clear instructions for handing over cases and defined guidelines. Regular inter agency meetings or working groups to discuss ongoing cases and share information.
	The NRW ERDF managing authority: Filing of criminal complaints due to suspected fraud.
DE	The Lower Saxony ERDF managing authority: Encrypted email system on Lower Saxony's secure federal-state network. The ESF Plus Federal Programme, led by the Federal Ministry of Labour and Social Affairs (BMAS): The reporting authorities usually file a criminal complaint and provide the documents

Member State	Response
	necessary for the judicial authorities' assessment. Moreover, Sections 406d and 475 of the Code of Criminal Procedure (StPO) regulate the relevant right of access to information. The Bremen ERDF managing authority: When a possible case of fraud is detected by the intermediate bodies, as is generally the case, they inform the managing authority and, at the same time, step up the administrative checks. If the suspicion is not confirmed, the intermediate bodies inform the managing authority accordingly. However, if the suspicion is confirmed, the intermediate bodies refer the case to the public prosecutor's office and inform the managing authority. Once the public prosecutor's office has come to a conclusion, the intermediate body is informed. In turn, the intermediate body informs the managing authority. The AMIF managing authority: In both our internal guidelines on handling irregularities and audit documentation, we have established a system for reporting cases of fraud to the competent Ministry of the Interior, our legal service, the public prosecutor's office and the European Commission (via IMS to OLAF). The roles of the bodies involved and the reporting channels are clearly defined. The Thuringia ERDF managing authority: Please see the ERDF guidance document and the 2025 manual on reporting irregularities in shared management. In accordance with the applicable national legal provisions, the implementing body or the authorising body must notify the public prosecutor's office accordingly, also informing the managing authority. A digital-only reporting process has been available since the end of January and is being tested.
DK	Danish Agricultural and Fisheries Agency: Systematic approach to when suspected cases are reported to relevant authorities. The Danish Agriculture and Fisheries Agency is always ready to assist the judicial authorities with information regarding irregular cases.
EE	In Estonia, criminal investigations are initiated by the implementing bodies responsible for project management, and they act as the primary contact point for the competent investigative authority (EPPO or the national prosecution service). AFCOS supports both the implementing bodies and the managing authority by facilitating information exchange at key stages — including the initiation of a case and the quarterly follow-up on its progress. Due to the EPPO Regulation and the internal information-sharing arrangements in place, AFCOS does not receive operational information directly from EPPO. As a result, the implementing bodies remain the main channel for communication with investigative authorities. AFCOS ensures an unhindered flow of administrative information by maintaining regular contact with the implementing bodies, providing guidance on reporting obligations, and consolidating the information required for OLAF and Commission reporting.
EL	Communication with: A) the office of the European Delegated Prosecutors, e.g. verbally, over email, via the distribution of printed information, B) national prosecution authorities.
ES	The Spanish AFCOS carries out information and monitoring functions for the classification and reporting of suspected fraud, informing the authorities of the existence of ongoing legal proceedings, as well as their completion, requesting information from the judicial bodies, all on the basis of the criteria contained in the document 'Criteria for classification and procedure for action regarding irregularities and suspected fraud in operations and projects that are the subject of criminal proceedings' issued by AFCOS. AFCOS has recommended that all managing authorities, when referring a case to the

Member State	Response
	European Public Prosecutor's Office, as well as when obtaining any updates on the case, communicate this to AFCOS so that it can monitor the correct communication in IMS, where appropriate, of suspected fraud. In this way, AFCOS can be aware of cases sent to the European Public Prosecutor's Office and request updates on their status. In the various training courses given, the importance of keeping the information in IMS and AFCOS up to date has been explained and highlighted so that AFCOS can monitor cases that have gone to court. There is a protocol signed with the National Police for collaboration and exchange of information with AFCOS, and the renewal of the protocol with the Civil Guard is currently pending signature. Under these protocols, requests for information are received, sometimes in the context of European Public Prosecutor's Office investigations, which allows the AFCOS to contact EPPO in order to obtain the necessary information to, where appropriate, proceed with communication in IMS. Any information obtained by AFCOS, either through IMS reviews or by other means, which involves a modification of communications is forwarded to the authorities responsible for it, with AFCOS monitoring the correct communication. There is also a protocol between the National Audit Office and AFCOS, both of which are part of the General State Comptroller (IGAE), relating to the exchange of information between the two units on cases of suspected fraud in the area of the Recovery, Transformation and Resilience Plan.
FI	The authorities responsible for implementing EU programmes exercise administrative powers. The legislation in each sector sets out the powers and duties of authorities to monitor activities and if necessary, carry out recovery. If an administrative authority has reason to suspect fraud, it makes 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 and Customs carry out criminal investigations in accordance with their powers, while prosecutors prosecute and the courts conduct the judicial process. Roles and powers are clearly 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. The administrative authorities do not hold these kinds of powers but provide the authority conducting the preliminary investigation with the necessary information in the investigation request.
FR	We are strengthening governance in the fight against fraud with a new architecture steered by the MICAF (the Interministerial Anti-Fraud Coordination Mission). This involves the interministerial unit for the anti-fraud monitoring of public funds and a number of national anti-fraud operating groups (groupes opérationnels nationaux anti-fraude - GONAF). For example: The interministerial unit for the anti-fraud monitoring of public funds, attached to the MICAF, will play a key role in dealing with fraud linked to European expenditure. With regard to the Recovery and Resilience Facility (RRF), this unit will coordinate dedicated working groups (WGs), particularly in the field of energy renovation and apprenticeships. The monitoring unit will also analyse the risks associated with implementing new European arrangements. In this new architecture, operational management relating to revenue fraud will be carried out by the GONAFs, co-facilitated by the MICAF, the DGFiP (Directorate-General for Public Finance) and the DGDDI (Directorate-General for Customs and Indirect Taxation). These groups will coordinate efforts to combat revenue fraud, such as fraud linked to VAT, e-commerce, tobacco and counterfeiting by drawing on strengthened information-sharing and risk-analysis mechanisms. We are improving the effectiveness of investigations led by the EPPO through better

Member State	Response
	coordination and improved stakeholder awareness; We are developing the role of the financial courts in order to make the fight against fraud affecting the EU's financial interests a more integral part of their investigations.
HR	Contribution from HR AFCOS unit: Enhanced cooperation between reporting and judicial bodies is ensured by adopting Decision on Establishing the AFCOS Network, which obliges AFCOS Network bodies (including judicial bodies) to exchange the information with the bodies of the management and control system for the use of funds of the European Union, the bodies of the management and monitoring system for the implementation of activities under the National Recovery and Resilience Plan 2021–2026, AFCOS Unit, and the European Anti-Fraud Office (OLAF). The first Decision was adopted in 2008, and the new one was adopted in 2025. Exchange of information may also take form of AFCOS Network meetings.
HU	The Internal Audit and Integrity Directorate acts as a single point of contact between the (reporting) managing authorities and the investigating authorities. The directorate monitors procedures initiated following suspicion of fraud and forwards the information obtained to the competent managing authorities and investigating authorities.
IE	The Irish AFCOS does not have a role in this space. It is for the government department/bodies managing EU funds to do so. They have stressed clear lines of communication with An Garda Síochána, or another appropriate civil authority, where an investigation of a suspected fraud has taken place.
IT	The managing authorities (MA) and the judicial authorities primarily exchange information through ordinary certified email channels, i.e. by way of the criminal investigation body performing the investigations (subject to prior authorisation from the prosecuting judicial authority).
LT	Direct communication.
LU	The information is first transmitted to the competent Minister. From there on, after a coordination discussion with the audit authority, a written denunciation letter, signed by the competent Minister would be sent to the EPPO and national jurisdictions.
LV	Reporting of suspicions of fraud to EPPO or national judicial authorities is carried out in accordance with regulatory enactments. In additions each ES funds authority have a contact person in EPPO with whom they can exchange information and receive consultations.
MT	The Maltese AFCOS is the reporting authority with respect to irregularities and cases of suspected fraud forwarded by the Managing Authorities, Paying Agency, Audit Authority and Certifying Body of EU funds (kindly refer to the reply provided in Question 1.6). Information flow with respect to suspected cases of fraud is dealt with by FID with judicial authorities, in terms of the Internal Audit and Financial Investigations Act (Cap. 461 of the Laws of Malta).
NL	There are set procedures that staff must follow if they suspect fraud when dealing with a project grant. As soon as further investigation shows that the suspicion is justified, an external party is contacted and informed. That party decides whether to pursue the matter and contacts the Public Prosecutor's Office and the EPPO. These procedures are also set out in writing.
PL	One such practice is the 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 cofinanced by EU funds:

Member State	Response
	- 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 to the institution; - Ongoing cooperation: exchange of information via a dedicated email address where it is necessary to obtain data on specific proceedings; - Direct referral of questions by managing authorities to individual public prosecutors' offices regarding specific ongoing proceedings. 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 case files 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 case files (including in digital form) is taken, in accordance with the relevant legislation, by the authority handling the case. Furthermore, an agreement is currently being prepared on the electronic transmission to organisational units of the Police of information collected in the CST2021 IT system, which supports programme implementation. In agricultural policy, each irregularity found is analysed individually in order to determine whether there is substantiated suspicion that the beneficiary has committed a crime or minor offence. Decisions on whether to refer a case to the law enforcement authorities and draw up a notice of substantiated suspicion that a crime/minor offence has been committed are taken by the competent administrative authority without undue delay. All cases referred to the law enforcement authorities are recorded in the in-house information system, with the stage that ongoing criminal proceedings have reached being indicated. If there is no information on the current stage of criminal proceedings being conducted by law enforcement authorities, a request for such information to be transmitted is sent to the authority conducting the case and the data is updated in the system. The data in the IMS report is then supplemented on the basis of the information received. For ongoing cases that are subject to reporting in IMS, quarterly verification is carried out until the criminal proceedings in the case have been completed.
	Information provided by OLAF or the EPPO (or both) is treated confidentially.
PT	The protocols for coordination with the judicial bodies establish secure mechanisms for sending information, and procedures and channels for national authorities to exchange information on irregularities.
RO	Clear rules for reporting suspected fraud cases. Designated persons responsible for communicating information. Use of specific systems for transmitting information.
SE	Communication and the dissemination of information take place via email.
SI	Regular contacts and communication and inter-ministerial group meetings.
SK	The process of reporting irregularities to OLAF involves several key steps, proceeding from the Managing Authority (MA) or Intermediate Body (IB) via the Certifying Authority/Paying Authority (CA/PA) to the AFCOS. The MA/IB is responsible for reporting the detected irregularity and for recording the information on the irregularity in the national IT monitoring system (ITMS). The MA/IB is responsible for resolving the irregularity. For this reason, the MA/IB receives information on all initiated and ongoing proceedings from the authorities

Member State	Response
	conducting criminal proceedings on the basis of the legislation governing the provision of information related to criminal proceedings by the police, the prosecution and the courts. These entities are obliged to provide the requested cooperation; it may only be refused if this could jeopardise the independent exercise of their statutory tasks. If the audit authority (AA) detects an irregularity on its own initiative and does not refer the matter to the implementing authority, it is obliged to issue a report on the detected irregularity via the ITMS. If a statutory body, an employee or a person acting on behalf of the MA/IB is suspected of having committed a criminal offence in connection with the implementation of the programme, a paper report on the detected irregularity is drawn up, approved and submitted to the CA/PA and AFCOS. The ITMS contains detailed information on the irregularity in question, on the basis of which the competent authority/CA/PA forwards their report to AFCOS and subsequently AFCOS reports the cases via IMS. There is regular communication and exchange of information (e.g. on legal procedures, technical procedures) between all the above-mentioned bodies. Where necessary, other bodies are also involved, such as the AA, law enforcement authorities, etc. In the case of agricultural funds, judicial authorities contact/inform the Agricultural Paying Agency (APA). The exchange of information then takes place as follows: APA via IMS to AFCOS. The exchange of information regarding fraudulent irregularities is based on a cooperation agreement between AFCOS and the General Prosecutor's Office of the Slovak Republic. On 18 December 2025, a new Memorandum of Cooperation was concluded between the Office of the Government of the Slovak Republic as AFCOS and the Ministry of the Interior of the Slovak Republic, specifically the Office for the Fight against organised Crime - UBOK, with the aim of strengthening cooperation in this area. AFCOS independently receives information on the initiation and final judgment (acquittal/conviction) of criminal prosecution against legal persons for a crime committed in connection with assistance and support provided from European Union funds in accordance with Act No. 91/2016 Coll. on the Criminal Liability of Legal Persons. The guidelines issued by the competent national authorities in the field of handling and reporting irregularities (in particular AFCOS and the Ministry of Finance of the Slovak Republic) set out a detailed procedure for processing and using the information provided on ongoing criminal prosecutions in order to ensure the continuous, active and effective protection of the financial interests of the European Union in the Slovak Republic and to improve the correct reporting of irregularities with qualifications IRQ3 and IRQ5.

Q.2.2 (AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? IMS

Response	Frequency	Percentage	Member States
Used	22	81.5%	AT, BE, BG, CY, CZ, DE, DK, EE, ES, FI, HR, HU, IT, LU, LV, MT,

Response	Frequency	Percentage	Member States
			PL, PT, RO, SE, SI, SK
Planned to Use	2	7.4%	LT, NL
Not Used	3	11.1%	EL, FR, IE

Q.2.2 (AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? Secure data exchange platforms (Online)

Response	Frequency	Percentage	Member States
Used	11	40.7%	CZ, DE, EE, EL, ES, HU, IT, LV, NL, PL, RO
Planned to Use	2	7.4%	BE, CY
Not Used	14	51.9%	AT, BG, DK, FI, FR, HR, IE, LT, LU, MT, PT, SE, SI, SK

Q.2.2 (AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? Shared case management systems

Response	Frequency	Percentage	Member States
Used	10	37.0%	CZ, DK, EE, ES, FI, FR, NL, PT, RO, SK
Planned to Use	3	11.1%	CY, EL, LU
Not Used	14	51.9%	AT, BE, BG, DE, HR, HU, IE, IT, LT, LV, MT, PL, SE, SI

Q.2.2 (AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? Encrypted email

Response	Frequency	Percentage	Member States
Used	15	55.6%	BG, CY, CZ, DE, DK, EE, EL, ES, FI, FR, LT, LU, NL, PL, PT
Planned to Use	1	3.7%	BE
Not Used	11	40.7%	AT, HR, HU, IE, IT, LV, MT, RO, SE, SI, SK

Q.2.2 (AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? Regular meetings

Response	Frequency	Percentage	Member States
Used	25	92.6%	AT, BE, BG, CY, CZ, DE, DK, EE, EL, ES, FI, FR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, RO, SI, SK
Not Used	2	7.4%	HR, SE

Q.2.2 (AFCOS) Which communication methods are used for coordination of your Anti-Fraud efforts? Other (please specify)

Response	Frequency	Percentage	Member States
Used	8	29.6%	AT, CZ, DE, ES, HR, IE, SI, SK
Not Used	19	70.4%	BE, BG, CY, DK, EE, EL, FI, FR, HU, IT, LT,

Response	Frequency	Percentage	Member States
			LU, LV, MT, NL, PL, PT, RO, SE

Following Q.2.2, please specify "Other".

Member State	Response
AT	The AFCOS is only a facilitator and coordinator and assists in OLAF's on-the-spot checks or audit requests from OLAF. In practice, OLAF makes contact by email.
CZ	Ad hoc meetings.
DE	The AMIF managing authority: The German managing authorities of the home affairs funds (AMIF, ISF and BMVI) use a common IT system (the ITS); however, there is no web-based fraud detection software as part of a common case management system.
ES	Protocols of cooperation between authorities
HR	- AFCOS Network meetings (meetings between MCS AFCOS Network bodies and AFCOS Unit) and meetings between AFCOS Unit and management and control system bodies which are organised when necessary - Irregularity Management Guidelines issued by AFCOS Unit and intended for MCS bodies - Written communication on specific issues
IE	AFCOS liaise with the country officers and reporting authorities on a regular basis. Quarterly meetings are held throughout the year, in addition to bilateral conversations as required. AFCOS plays the role of the URT-liaison officer for all reporting authorities and will update the user list on a quarterly basis.
SI	Conferences, annual meetings.
SK	Paper form in case the person acting on behalf of the implementing authority would be suspected of committing a criminal offense.

Q.2.3 (All entities involved with fraudulent irregularities) If your Member State uses secured online platforms or shared case management systems, roughly, what percentage of fraudulent irregularity cases are processed and followed up primarily through these digital channels (as opposed to paper or conventional correspondence)?

Response	Frequency	Percentage	Member States
76–100%	13	48.1%	CZ, DE, EE, EL, ES, FI, IT, LV,

Response	Frequency	Percentage	Member States
			NL, PL, PT, RO, SK
26–50%	2	7.4%	DK, FR
51–75%	1	3.7%	HU

Q.2.4 (IMS users) Which IMS fields prove the most difficult to receive accurate, complete, and timely information for?

Member State	Response
AT	n/a
BE	ESF VL EUROPA WSE: The problem is that the fields change over time. Sometimes we have to add information for projects that are already closed.
BG	In rare cases, it is difficult to precisely determine the amount affected by the irregularity
CY	Categorization/classification of irregularities, persons concerned, relevant EU provisions.
	Field 6.9
	Fields 6.3, 6.4, 6.7, 6.8, 7.2 and 7.3
CZ	Field 8.5: Police progress reports on criminal investigations are either late or we do not receive them at all, making it difficult to provide information in this field. Annexes - for example, judgments with a jurisdiction clause and data from insolvency and enforcement proceedings.
	The Lower Saxony ERDF managing authority: All mandatory fields can be completed with the available information.
	The EU Paying Agency for Lower Saxony, Bremen and Hamburg: No 2.2.2 'Function or role'.
	The Schleswig-Holstein ERDF managing authority: It is most difficult to obtain information for IMS fields 6.7.1 and 6.7.2 (Irregularity committed from/to).
DE	The Bremen ERDF managing authority: No 3.11 'Definition of the priority axis'; No 3.12 'Definition of the operation'; No 6.8 'Determination of the type of irregularity'. For each of the above-mentioned fields, the applicable criteria should be selected from the drop-down lists provided. These correspond only vaguely to the actual programme structures and irregularities detected. The best possible choice must be made. The AMIF managing authority: Category No 6 in the IMS, 'Type of irregularities', since, often, not enough information is available. Obtaining information is often time-consuming. The Federal Office for Agriculture and Food (BLE):

Member State	Response
	2.1.2 'National identification number', 2.1.3, 2.1.4: as a rule, this information is not requested in advance, for example identity cards or the like do not have to be presented for aid to be granted, and the holding number is not necessarily requested if the aid is not area aid under direct payments. 2.1.7 'Parent company'. The Baden-Württemberg managing authority: 3.11 'Priority axis' and 3.12. 'Operation(s)', as this priority axis, which underlies the programme, is not available. 6.8.1–6.8.3 'Detailed information on the irregularity': here too the options do not correspond to reality / it is difficult to classify specific projects. In general, the fact that fields 3.11 and 3.12 and 6.8.1 to 6.8.3 are mutually dependent poses a challenge, as, while the selection made in the first field is not necessarily appropriate, it is necessary in order to reach the more precise options in the following fields.
DK	Danish Business Authority: - The financial scope (amounts involved and amounts recovered) as this information is often only available as preliminary assessment at the time of the first report and may change as further checks, administrative decisions and possible amounts are recovered. - Classification of the irregularity, including the assessment of whether it is a case of suspected fraud, since the final classification often only can be determined after further examination and possible investigation. - Administrative and legal follow-up since the necessary information to fill in the required fields often relies on information from other authorities.
EE	For us, the most time-consuming item is IMS field 6.1 (the date on which the information was received that led to the suspicion that an irregularity had been committed). This information has to be identified from multiple sources and cannot be retrieved automatically.
EL	Field 10 on the development of court decisions. More specifically, judicial authorities do not inform the reporting authorities of any notified cases of suspected fraud. Consequently, the reporting authorities cannot update these cases.
ES	- Details of the projects and operations affected by the irregularity. - Obtaining information on ongoing or open cases, given the confidential nature of such proceedings, which would affect IRQ3 communications. - Obtaining final judgments and the information to be included in IMS for IRQ5 communications. - Information for updating fields 9 on actual repayments
FI	Sanctions are the most challenging fields, as judicial processes typically take a long time.
FR	The cancellation of an irregularity following a court decision removes all or some of the data already entered in IMS, in particular the <i>modus operandi</i>, which makes it difficult to trace operations.
HR	Contribution from the Ministry of Agriculture, Forestry and Fisheries (Paying Agency for Agriculture, Fisheries and Rural Development): Case update field, in the case where refund is requested from the user, the refund process sometimes takes a long time, which can make it difficult to update in a timely manner. Contribution from the Ministry of Agriculture, Forestry and Fisheries, Directorate of Fisheries: Fields on classification of irregularity as "suspected fraud" and/or "fraud", taking into account that such information should come from judicial authorities. Contribution from the Ministry of Labour, Pension System, Family and Social Policy: 4.3 Total amount of irregularity 8.2 Amount of irregularity

Member State	Response
	8.2.1 whereof not paid 8.2.2 whereof paid 9.5 Amount recovered 9.14 Recovery measures already taken 10.5 Status of procedure 10.6 Sanctions Contribution from the Ministry of Regional Development and EU funds: Section 10 of the IMS (Sanctions) – information on reported fraud to the State Attorney's Office of the Republic of Croatia and EPPO and actions taken or proceedings initiated is provided only on request and in a very limited scope. The proceedings themselves take a very long time, so there are long periods when there is no information to report. The same situation applies to criminal/civil court proceedings – some cases are pending for a very long time, and information on the progress of the proceedings is not available. For the IMS users the most difficult task is obtaining accurate, complete, and timely information for the following system points: 2.2. NUTS levels The system does not allow a single User to select multiple NUTS regions. 3.11. Priority and 3.12. Theme The options offered in the IMS are not consistent with the Decision on Irregularity form 4.1.4. Expense amount and 4.1.5. Irregularity amount – difficulties occur when entering data due to dependency on data given by other employees, which can sometimes be contradictory and inadequate. 6.9. Modus operandi A large portion of the data that would cover Modus operandi as in the Decision on Irregularity is also entered in point 11. Comment: it should be clarified in more detail what is entered where. 8 and 9 Everything regarding the amount and refund, as it depends on data employees provide, as well as 4.1.4 and 4.1.5.
HU	The programmes' national monitoring system provides accurate and timely information for completing the IMS. In cases of suspected fraud, due to the time needed to conduct criminal proceedings, the final information is available only after a lengthy period, which has an impact on the completion of the Type of irregularity, Modus operandi, Classification of the irregularity and Sanctions fields.
IE	6.8.1 Category 6.8.2 Type 6.8.3 Type of irregularity 6.9 Modus operandi
IT	There have not been any issues in any of the areas.
LT	To date, the financial crime investigation service does not yet have access to this system but will soon.
LU	N/A

Member State	Response
LV	Problematic receipt of timely information in cases where information is received from investigative authorities (e.g., IMS fields 6.1., 6.7., 7.1.)
MT	No difficulties are encountered due to continuous communication with the Managing Authorities, Paying Agency, Audit Authority and Certifying Body of EU funds.
NL	For the PA, the system provides the possibility to update the fields, and additional information can therefore always be added until a case is closed. Constantly keeping track of this information is time-consuming, which makes it particularly difficult.
PL	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 that sent the notice of a possible criminal offence.
	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 those personal data of a convicted natural person that must be included in the IMS reporting form. This is because in their judgments, courts do not always include information such as the personal identification (PESEL) number or the registered residence address of the person concerned. Particularly long criminal cases, i.e. those whose duration significantly exceeds the financial perspective concerned, constitute a separate category of case. Another problematic issue is how to properly reflect the type of criminal penalties imposed by courts using the list of options available in IMS (tab 10).
PT	6.7 Irregularity committed on / between; 6.8 Type of irregularity e 6.9 Modus operandi.
RO	Procedures/sanctions
SE	We do not see any difficulties in this regard.
SI	The date when a suspicion of fraud was detected.
SK	Fields in Chapter 10 – Sanctions. For CAP - fields related to other proceedings (judicial, criminal proceedings) and fields related to the nomenclature of individual payment requests.

Q.2.5 (All entities involved with fraudulent irregularities) How do you try to balance the confidentiality of investigations with the necessity to report?

Member State	Response
AT	Austria has clear legal rules on data protection and confidentiality and the need to report.
BE	PSW ERDF Wallonia: (PSW) Access to information is restricted and only OLAF representatives or people in charge of collecting reports know the contents of the file in order to prevent any data leak. At the level of investigations within the administration, only the people in charge of

Member State	Response
	investigations are informed of the contents of the file. Reports are made by means of a platform for reporting irregularities, via the integrity officer, or via the OLAF Working Group. At the level of the judicial authorities, only the people who submit the files and the judges in charge of the investigation know the contents of the file. They are communicated to the judicial authorities by official report. ERDF and RRF Brussels Capital Region: It is a question of weighing up the principle of confidentiality against the duty to report, complying with the rules and guidelines on reporting and applying the principle of data minimisation (whereby an objective is to be achieved using as little confidential or sensitive information as possible). EUROPA WSE (ESF VL): Investigations are performed by different colleagues than the personnel of ESF Flanders (VSI instead of Europa WSE). As such confidentiality is mostly contained within their investigations, while we only receive the results.
BG	In accordance with national legislation and methodological guidelines issued by the AFCOS Directorate, the reporting organisations shall promptly report the information that has become known to them through the investigations initiated
CY	Only dedicated staff is involved in reporting; information is saved in locked folders accessible only to dedicated staff. The reporting duty is only assigned to the dedicated team.
CZ	Official investigations are usually conducted under legislation such as the Control Code and the Tax Code, which include confidentiality obligations for investigators. The same confidentiality arrangements apply to law enforcement authorities. The confidentiality of investigations is thus guaranteed by confidentiality obligations. Communication without undue risk of exposure to persons without authority or jurisdiction. By limiting the number of interested parties, and by passing on information according to the rules (Code of Ethics). Notifications are issued only by selected staff. Documents and information relating to an investigation are never stored on a shared disk; they are cloud-based (SharePoint) and accessible only to the staff involved in the investigation. This means that information flows in a timely and secure manner. We achieve an appropriate balance between ensuring the confidentiality of investigations and reporting obligations through strict compliance with the rules and robust protection of sensitive data. Upon request, the managing authority (MA) provides the law enforcement authorities with all the necessary documentation. Once the case has been transferred the MA fully respects the confidentiality of the criminal proceedings and is prohibited from any form of involvement therein. Communication may take place provided it does not undermine the investigation or the rights of those concerned. As such it is possible to comply with the legal obligation to report serious suspicions of fraudulent conduct without prejudice to the integrity of ongoing investigations, for which the law enforcement authorities have sole responsibility.
DE	The Lower Saxony ERDF managing authority: All the necessary information is already requested as part of the ongoing funding process. Where there are reasonable grounds to suspect fraud, the investigation is referred to the competent public prosecutor's office.

Member State	Response
	The EU Paying Agency for Lower Saxony, Bremen and Hamburg: Secure data exchange through data exchange platforms. The ESF Plus Federal Programme, led by the Federal Ministry of Labour and Social Affairs (BMAS): Access to OLAF is restricted to a selected group of people. The Schleswig-Holstein ERDF managing authority: Confidentiality between the bodies involved is guaranteed by having separate systems. The Bremen ERDF managing authority: Beneficiaries submit a list of all supporting documents to the intermediate bodies when making payment claims. A sample is taken from this list. Accordingly, the individual supporting documents are requested and made available electronically to the intermediate bodies. If suspicions of possible fraud arise in the context of the administrative check, the sample is enlarged and additional supporting documents are requested. If the suspicions are confirmed, a report is made to the public prosecutor's office. At the same time, the managing authority is informed. The AMIF managing authority: As regards reporting to national bodies (ministries, supervisory authorities, public prosecutor's offices), confidentiality is ensured by various national rules in laws, guidelines and control systems. Moreover, the number of people who are privy to the information should be as low as possible and limited to what is necessary. Hence the respective responsibilities of the employees are clearly defined and restricted. Staff are instructed not to disclose information to unauthorised persons. In the ITSI IT system for home affairs funds, it is ensured that beneficiaries can only view information on the projects that they have made an application for and are to carry out. The Thuringia ERDF managing authority: Investigations are carried out as part of the examination of documents or, where applicable, consultation procedures or preliminary checks with short or medium time frames. It is also possible to report suspicions anonymously. The Brandenburg ERDF managing authority: Confidentiality obligation, sensitive handling of data, reporting and activities undertaken by competent persons only (very small group).
DK	Danish Business Authority: Balance is ensured by reporting in IMS at an overall and factual level without sharing information that could negatively impact ongoing investigations. Reporting is based on available information and updated when it is possible to share new information, taking into account confidentiality. Danish Agricultural and Fisheries Agency: To remain vigilant in providing necessary information to relevant authorities and protecting information in accordance with GDPR.
EE	We balance the confidentiality of investigations with reporting obligations by strictly following the legal framework governing access to investigative information. Criminal investigations are handled by the competent investigative prosecutor, who determines what information can be shared with other authorities. As a result, Estonian authorities do not receive operational details that could compromise confidentiality. Reporting is therefore based solely on information that can be disclosed without affecting the investigation, and we rely on the implementing bodies to provide the elements that may be shared. This approach ensures that sensitive investigative information remains protected, while

Member State	Response
	Estonia can still meet its reporting obligations to OLAF and the Commission using verified, non-confidential data.
EL	In such circumstances, it is stated that the case is under investigation, so any information is limited to details that are strictly necessary and do not affect the audit of the case.
ES	Through a thorough analysis of each case and the identification of those allegedly affected. This process makes it possible to determine what information is essential for the intermediary bodies, while protecting the integrity of the investigation and the privacy of the individuals involved, seeking a middle ground where transparency does not compromise the effectiveness of the investigation or cause unnecessary harm to third parties. Likewise, by eliminating irrelevant personal data, referring to the obligation to comply with personal data protection regulations and using passwords to open files, as well as by transmitting communications through internal systems, such as the Civil Guard's Internal Investigation Management System. In the case of the AFCOS Infofraude reporting channel, which is intended to receive information on fraud, irregularities or any other illegal activity affecting the financial interests of the EU, as well as the internal information channels of some authorities, reports may be submitted anonymously. For those whistleblowers who decide to report non-anonymously, the application of Law 2/2023 of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, is guaranteed. In the case of non-anonymous reports, the confidentiality of the whistleblower's identity is guaranteed, so that it will not be disclosed to anyone. To this end, in all communications, verification actions or requests for documentation carried out by AFCOS, data relating to the identity of the person who submitted the information, as well as any other data that could lead to their total or partial identification, will be omitted. Confidentiality clauses are also included in all written requests for information that are sent. In the case of irregularities detected and reported in the first instance by the authorities responsible for fund management, which have been referred to the European Public Prosecutor's Office by them, there would in principle be no confidentiality issues because most of the data is known to those authorities for communication purposes. In cases other than these, when AFCOS becomes aware of an investigation by the European Public Prosecutor's Office and requests information for communication purposes via IMS, it is the European Public Prosecutor's Office that decides what data it can or cannot provide.
FI	Reporting focuses only on the necessary data; data protection and data security are ensured.
FR	If an irregularity with an intentional element is found during an investigation, Article 40 of the Code of Criminal Procedure requires that this irregularity be reported to the competent public prosecutor's office.
HR	Contribution from the Ministry of Agriculture, Forestry and Fisheries (Paying Agency for Agriculture, Fisheries and Rural Development): Data is updated respecting data entry by authorised IMS users. Contribution from the Ministry of Agriculture, Forestry and Fisheries, Directorate of Fisheries: We include as much as possible information on irregularity, which is detected by administrative authorities, excluding only confidential information as instructed by authorities that are conducting investigation. Contribution from the Ministry of Regional Development and EU funds: In most cases, this is not a problem, since we only receive specific information after the

Member State	Response
	confidential actions are completed, so limited reporting through IMS does not represent a violation of confidentiality. Certain information that we find out while the action is in progress is usually not relevant for reporting. In exceptional cases, we would try to report confidential information through a general note without violating confidentiality, and in the case that this exact information it is extremely important for reporting - the request should be sent directly to the competent authority for approval of reporting.
HU	When the judicial body informs the reporting authority about proceedings relating to a fraudulent case, it is then possible to record it in the IMS.
IE	This varies on a case-by-case basis. Generally, stakeholders are only informed on a need-to-know basis.
IT	The balance between the confidentiality of investigations and the need for reporting is ensured (subject to formal authorisation by the prosecuting judicial authority) through the transmission of essential information in a proportionate and timely manner, in compliance with confidentiality constraints, the duty of investigative confidentiality and data protection legislation. Reports are updated periodically, providing additional information as soon as it is compatible with the progress of the investigation, in close coordination with the competent authorities. In the event of pending criminal proceedings, the judicial authorities are continually informed of the need to provide updated data, in part because the characterisation of the irregularity could be changed.
LT	We trust our partners, so we always report violations when we see them without compromising our investigation (in case of an ongoing investigation).
LU	As soon as a suspicion of fraud rises it will be reported to the judicial authorities. The confidentiality would not play a role.
LV	Reporting is carried out in accordance with the EPPO guidelines and in compliance with the requirements set out in regulatory enactments. Regarding internal investigations, a clear separation between internal investigations and mandatory reporting has been assessed and established, through initial fact-finding and assessment.
MT	As explained in Question 1.6, a quarterly Irregularity Reporting Sub-Group meeting is held to ensure correct and complete reporting of irregularities and suspected cases of fraud in line with standing reporting obligations.
NL	We anonymise the information.
PL	Reporting institutions have guaranteed access to the minimum information necessary to carry out their duties, with the confidentiality of proceedings being maintained. A key aspect is to maintain balance, i.e. for the authorities to send only the information necessary to complete the tasks without disclosing evidentiary details or sensitive data.
PT	Cases of irregularity with signs of fraud are reported, provided there is no confidentiality clause (on the key elements of cases) that may block such reporting. All detected cases of irregularity with signs of fraud are covered by the confidentiality clauses laid down in the particular administrative act to which the handling of a case is subject. If, during the correction process, the judicial body imposes another level of confidentiality, that new level becomes applicable immediately.
RO	Compliance with regulations on the confidentiality of criminal investigations. Requesting authorisation to report on a case-by-case basis

Member State	Response
SE	Ongoing registered cases are kept confidential in the registration system. The parties involved in the proceedings are informed.
SI	Recovery and Resilience Office: We proceed in line with the guidelines of the law enforcement bodies. Irregularity reports include only information that does not jeopardise investigations. The MKRR explains: Basic information on the suspicion of fraud detected is always provided/reported. Other information that has come to light by the time the irregularity is closed is provided at that stage.
SK	We receive only the amount of information required to meet the reporting rules of the IMS. This information does not include any sensitive information or operational details related to investigation.

Q.2.6 (AFCOS) How does your system enable timely follow-up to cases in IMS?

Member State	Response
AT	In Austria, the AFCOS is set up purely as a coordination body. It does not have any investigative powers of its own in the area of funding. However, each responsible department has an audit authority and a paying body. Each department is obliged to report irregularities for each fund. It is therefore not possible for Austria's AFCOS to track cases in IMS. Data entered in IMS is available / retrievable at any time
BE	Belgian AFCOS: Recently the role of country officers within the IMS system has been taken up by the Secretariat of the BE AFCOS. It is still up to the partner authorities to report their irregularities directly into the system. If there are data quality issues, we contact our respective liaison officers ensuring an update of the data surrounding these irregularities. PSW ERDF Wallonia ERDF, JTF and RRF at the PSW level: 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. The processes for reporting internal and external irregularities were put in place in 2023. The procedures for processing and rectifying irregularities or the integrity officer's procedure for internal fraud management as part of the internal reports are being drawn up.

Member State	Response
	The ESF Agency takes part in the OLAF Working Group chaired by the PSW and contributes to its work for the ESF and AMIF programmes.
BG	The national legislation and the methodological guidelines issued by the AFCOS Directorate precisely describe the grounds for creating a follow-up notification for tracking cases in IMS. Employees from the reporting organisations are periodically trained on these rules and an opportunity is created to discuss emerging issues and cases
CY	Irregularities deducted nationally are first withdrawn from EU funding and then reported to IMS so therefore no follow-up is required.
CZ	By continuously assessing the data in the IMS, identifying any deviations and critical states, observing trends and evolution; possibility of rapidly updating data. Procedures are in place for certain activities such as the continuous updating of cases and their enforcement. Prevention also works insofar as individual errors are analysed in terms of their potential impact on other funds, other related projects, etc. In such cases, an on-site public administrative check may take place and, if necessary, the project may be suspended, and the grant may even be withdrawn. Monitoring in IMS, regular reporting; those responsible monitor the status of open cases. Compliance with established internal procedures in accordance with the timelines set in internal guidelines and legislation.
DE	The Lower Saxony ERDF managing authority: Reporting deadlines have been set for relevant cases. The Bremen ERDF managing authority: The managing authority records reportable irregularities in the IMS within two months of their detection. If an attempt at fraud is confirmed by the public prosecutor's office, the original alert is adjusted accordingly. The AMIF managing authority: The complete recording of cases in the IMS always takes place in a timely manner, in accordance with the requirements set out in the manual on handling irregularities and the IMS guidance document, our management and control system and our internal guidelines. This recording is monitored by our supervisory authority, the Federal Ministry of the Interior (BMI). Comments and amendments by the BMI are always taken into account and incorporated. The Thuringia ERDF managing authority: Reconciliation of irregularities on a monthly basis and where necessary.
DK	Danish Business Authority: We manually follow up on cases both internally and with relevant authorities to ensure that new information is registered as soon as possible. Danish Agricultural and Fisheries Agency: Effective communication with other relevant administrative authorities in the reporting process.
EE	Estonia ensures timely follow-up to cases in IMS through national case-management systems, where all irregularities are processed in accordance with established procedures. Each case is monitored throughout its lifecycle, and implementing bodies are responsible for ensuring that all necessary steps are taken without delay. Once national procedures progress, the relevant information is uploaded to IMS. IMS is updated on a quarterly basis, in line with the Commission's reporting requirements.

Member State	Response
	Because the primary case handling takes place in secure national databases, follow-up actions are carried out promptly, and IMS is updated systematically based on the developments recorded in the national systems.
EL	The Greek AFCOS does not monitor cases in the IMS. This falls within the remit of EDEL and the Ministry of Rural Development and Food.
ES	A quarterly check is carried out by cross-referencing all data relating to IRQ3 and IRQ5 reported in IMS and requests for relevant, discrepant or necessary information. Any changes detected in relation to the previous quarter are consulted with the relevant authority to verify their origin, requesting correction if necessary, and following up on this. Any update to information known to AFCOS through any channel, which involves a change in IMS, is communicated to the authority responsible for such communication and is followed up until the update is confirmed in IMS.
FI	All the essential information relating to suspected fraud and irregularities and their current status is stored in the system.
FR	The AFCOS is not responsible for such follow-up in France.
HR	Contribution by the Croatian AFCOS unit: The AFCOS unit has developed guidelines on the management of irregularities for the authorities of the management and control system for the use of EU funds. The guidelines set the time limit for complying with the obligation to submit initial and follow-up reports to the AFCOS unit, which then checks the quality of the reports submitted. If corrections need to be made, the AFCOS unit sends the reports back to the reporting authority, giving appropriate instructions. The guidelines also state that, on a quarterly basis, the person responsible for the irregularity case must check whether new circumstances have arisen in relation to the case reported and, if so, draw up a follow-up report in the IMS system.
HU	Reporting authorities typically fulfil their follow-up obligation by regularly checking the information in their own records. It is also worth noting in relation to IRQ3 cases that there is a single-channel exchange of information between the development policy institutional system and the investigating authority, which also helps ensure that IMS data are up to date.
IE	AFCOS have quarterly network meetings where the need for all reporting authorities to follow-up on cases is stressed.
IT	The alert management system allows for timely follow-up of cases through a detailed and exhaustive preliminary assessment and investigation phase, as well as a continuous focus on the progress of the procedures launched. If this analysis reveals critical issues, information anomalies or significant risk elements, the necessary investigations and information flows to the competent authorities and bodies are promptly activated, ensuring the traceability of the activities carried out and the timely adoption of the resulting measures.
LT	To date, the financial crime investigation service does not yet have access to this system but will soon.
LU	The audit authority handles the IMS.
LV	AFCOS is not involved in reporting / following-up cases in IMS. Each EU funds authority performs these functions independently.
MT	Through coordination with the Managing Authorities and Paying Agency of EU funds.

Member State	Response
NL	Further developments in irregularities or suspicions of fraud are always recorded promptly in IMS. AFCOS: IMS is not yet being used. We are currently taking the administrative steps to organise this.
PL	The process of reporting irregularities to the Commission in IMS is coordinated and organised by the national AFCOS, which is responsible, among other things, for developing the national procedure, i.e. a set of compulsory rules for the individual reporting institutions, including as regards the updating of cases. The AFCOS regularly monitors the status of cases reported to the Commission in terms of whether they can be updated or closed. In cooperation with individual reporting institutions, it also takes specific measures to ensure that the information from Poland concerning individual reports is as up to date as possible. The approaches adopted by the competent institutions allow the timely notification of the follow-up actions in the cases reported in IMS, thanks mainly to inter-institutional cooperation that allows up to date information to be obtained as necessary. Such cooperation takes place, for example, on the basis of the cooperation agreement between the National Public Prosecutor and the minister responsible for regional development governing the transmission of information on ongoing and concluded proceedings concerning projects cofinanced by European funds. In addition, institutions carry out periodic reviews of cases, monitoring on an ongoing basis the follow-up actions in the proceedings being conducted.
PT	Procedures and mechanisms are in place for sending the information needed to follow up cases reported to OLAF.
RO	Periodic follow-up / clear procedures for monitoring cases / interinstitutional communication
SE	OLAF reports are registered and are available on the authority's common file space.
SI	Regular, timely reporting in place.
SK	Our system enables timely follow-up to cases in the IMS through regular notifications, defined case processing deadlines, clearly assigned responsibilities, and regular monitoring of case status. Cases are continuously updated, tracked with status indicators, and escalated to the appropriate management level in case of delays. Deployment of the "Reports to OLAF" module enables the AFCOS to export reported irregularities from ITMS2014+ and ITMS21+ to the IMS system export irregularities to OLAF's IMS platform. AFCOS regularly obtains information about initiated, ongoing and completed criminal proceedings based on the Cooperation Agreement concluded with the General Prosecutor's Office of the Slovak Republic, the Ministry of the Interior of the Slovak Republic and on the basis of the Act No. 91/2016 Coll. on the Corporate Criminal Liability. MA/IB/AA/CA/PA regularly informs AFCOS in accordance with the procedures and rules of the process for reporting irregularities, including their updates, set out in the Manual for Reporting Irregularities issued by AFCOS.

Q.2.7 (AFCOS) In which areas of reporting have you encountered problems when creating or updating cases? Cooperation with national administrative bodies

Response	Frequency	Percentage	Member States
Minor issues	3	11.1%	BE, CY, ES
No issues	24	88.9%	AT, BG, CZ, DE, DK, EE, EL, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, RO, SE, SI, SK

Q.2.7 (AFCOS) In which areas of reporting have you encountered problems when creating or updating cases? Cooperation with national investigative bodies

Response	Frequency	Percentage	Member States
Minor issues	7	25.9%	CZ, DK, EL, HR, HU, PL, SK
Serious issues	2	7.4%	CY, ES
No issues	18	66.7%	AT, BE, BG, DE, EE, FI, FR, IE, IT, LT, LU, LV, MT, NL, PT, RO, SE, SI

Q.2.7 (AFCOS) In which areas of reporting have you encountered problems when creating or updating cases? Cooperation with international administrative bodies

Response	Frequency	Percentage	Member States
Minor issues	1	3.7%	PL
Serious issues	1	3.7%	ES
No issues	25	92.6%	AT, BE, BG, CY, CZ, DE, DK, EE, EL, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL,

Response	Frequency	Percentage	Member States
			PT, RO, SE, SI, SK

Q.2.7 (AFCOS) In which areas of reporting have you encountered problems when creating or updating cases? Cooperation with international investigative bodies

Response	Frequency	Percentage	Member States
Minor issues	3	11.1%	EL, PL, SK
Serious issues	2	7.4%	CY, ES
No issues	22	81.5%	AT, BE, BG, CZ, DE, DK, EE, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PT, RO, SE, SI

Q.2.7 (AFCOS) In which areas of reporting have you encountered problems when creating or updating cases? Other (please specify)

Response	Frequency	Percentage	Member States
Minor issues	1	3.7%	IE
Serious issues	2	7.4%	EE, ES
No issues	24	88.9%	AT, BE, BG, CY, CZ, DE, DK, EL, FI, FR, HR, HU, IT, LT, LU, LV, MT, NL, PL, PT, RO, SE, SI, SK

Following Q2.7, please specify "Other".

Member State	Response
EE	The main reporting difficulties arise in relation to cases under EPPO investigation. Due to the EPPO Regulation, AFCOS does not receive operational information on EPPO-led investigations. This means that Estonia cannot access the details needed to create or update IMS cases beyond the limited information that implementing bodies are allowed to share. As a result, reporting on EPPO cases is constrained by the strict confidentiality rules that prevent the transmission of investigative information to AFCOS.
ES	Cooperation and exchange of information with judicial authorities
	Saying 'minor issues' solely to add narrative here.
IE	AFCOS have consulted with each reporting authority, and the feedback received stressed good cooperation with all of the above-mentioned stakeholders. The cooperation involves the reporting authorities. AFCOS has a limited role.

Q.2.8 (AFCOS) Please feel free to share any additional thoughts or experiences you have regarding the topics discussed in this section or support you require from the Commission/OLAF regarding them.

Member State	Response
AT	Each department (in Austria, seven departments are involved) is obliged to report irregularities and provide reports for the respective fund.
BE	Belgian AFCOS: Currently a lot of information concerning IMS is posted in the ALIB library. This library contains a high number of guidelines, instructions, ...that in reality partners get lost in the sea of documentation. We would like to obtain one pager's summarizing the necessary steps to ensure compliance with the set-up created by OLAF. This will help to boost quality levels of cases throughout the network.
	The Lower Saxony ERDF managing authority: The future systems (e.g. Arachne+) should be mandatory in the light of extensive testing phases and information. Up-to-date information on new developments in the IMS reporting process.
DE	The ESF Plus Federal Programme, led by the Federal Ministry of Labour and Social Affairs (BMAS): Unfortunately, the OLAF IMS is not self-explanatory. Mandatory fields are not adequately described. Dependencies are inadequate, so there is a regular need for revision. The search function is limited.
	The Thuringia ERDF managing authority: OLAF's feedback is rather lengthy. The reporting channels from OLAF to other units of the European Commission are not very transparent.
EE	Estonia would welcome further support from the Commission and OLAF in areas where national authorities face structural limitations, particularly regarding EPPO-led investigations.

Member State	Response
	While the current guidance is clear and workable, we see a need to further harmonise IMS pick-lists and their practical use across Member States. More consistent definitions and clearer distinctions between categories would improve comparability and enhance the value of OLAF's analyses. In addition, pick-lists should be aligned with those used by other Commission services (for example, EC auditors) to ensure coherence across different reporting and control systems and to avoid parallel or inconsistent classifications. We would also welcome the creation of a dedicated working group or network for IMS Country Officers. Such a platform would support regular exchanges, promote consistent reporting practices, and strengthen cooperation between Member States and OLAF, especially in areas where national approaches differ or where reporting is affected by external constraints.
EL	The new revision of Regulation (EU, Euratom) No 883/2013 should stipulate that national anti-fraud strategies in the Member States will be drawn up exclusively by the AFCOSs.
	There are a number of irregularities that are sometimes not reported or are reported late, and which AFCOS is unable to follow up properly, such as: - Irregularities reflected in OLAF reports. The reports are not received by AFCOS, which means that it cannot follow up either the IMS communication or the adoption of corrective measures. One possible improvement would be to inform AFCOS when the Commission sends the Member State the OLAF recommendations and report, so that it can follow up on the corresponding communication. - Cases referred by OLAF to the European Public Prosecutor's Office. No information is obtained on these cases. In order to improve communication, it would be advisable for OLAF to notify AFCOS of cases that it has referred to the European Public Prosecutor's Office, so that these can be followed up and communicated appropriately. If, for reasons of confidentiality, this cannot be done at the initial stage, it could be done at a later stage of the proceedings, such as at the start of the trial phase.
ES	Furthermore, a common point of contact could be created between AFCOS, OLAF and the European Public Prosecutor's Office to facilitate the exchange of information, also for the purposes of communication in IMS, given that on occasions the same information is received by the three institutions without there being proper coordination. It would be desirable for the Commission to standardise protocols and issue clear guidelines for the purposes of communication and information. One way of achieving complete and accurate communications within the deadline would be to establish some form of penalty for non-compliance, including financial penalties, depending on the seriousness of the breach and in accordance with the principle of proportionality.
HR	Contribution by the Croatian AFCOS unit: The authorities of the management and control system for the use of EU funds have difficulties in obtaining timely information on cases in which criminal proceedings have been initiated, because Croatian legislation imposes restrictions on the disclosure of such information. Additionally, the prolonged duration of most criminal proceedings further complicates the follow-up and closure of cases.
HU	In order to promote uniform reporting at EU level, we recommend organising professional events focusing on the interpretation and practical application of EU legislation and OLAF guidelines.
IE	Data sharing/GDPR compliance is a significant issue that requires clarity and the need for a unique national identifier is a significant obstacle to coordinating anti-fraud measure This can limit the effectiveness of the use of Arachne.

Member State	Response
IT	It would be useful if the European judicial authority were to inform the administrative authorities responsible for managing the relevant European funds as soon as possible in cases of suspected fraud under investigation, within the limits permitted by the applicable legal framework and in accordance with the requirements of confidentiality and due regard for the confidentiality of investigations. Moreover, this information would be particularly helpful at the conclusion of ongoing investigations in cases where the managing authority could not otherwise have detected the case of suspected fraud. In such circumstances, notification from the judicial authority may be the only means by which the managing authority was in a position to carry out the activities within its remit, including alerts in the IMS-OLAF system. The timely transmission of this information would also allow the case to be handled properly, efficiently and quickly, including from an administrative point of view, in line with the responsibilities assigned to managing authorities under the programmes financed by the European Union.
NL	No further comments.
PL	Questions 1.2 and 1.4 are identical. It has been assumed that question 1.4 concerns the part of the anti-fraud cycle in which the institutions' actions have had the least effect, and this is how the answer was approached.
PT	The national administrative bodies have been very cooperative, providing a great deal of information for the investigations conducted by OLAF and the national judicial bodies.
SK	AFCOS welcomes the continued support from the Commission and OLAF in improving the quality and timeliness of case reporting in the IMS. In particular, we consider the new version of the Handbook on "Reporting of irregularities in shared management" to be especially beneficial. We also positively assess initiatives aimed at the exchange of best practices among Member States and the workshops organised by OLAF, which significantly contribute to enhancing the professional capacities of the authorities involved.

RECOMMENDATION 4 – DIGITALISATION AS A PILLAR OF THE NATIONAL ANTI-FRAUD STRATEGY

The Commission reiterates its call to national authorities to embed the digitalisation of the fight against fraud in their national anti-fraud strategies, with the aim of: a) assessing the level of threat posed to the EU budget by the rise in cybercrime and the use of AI and other innovative technologies, in particular by organised crime; b) identifying their knowledge and skill gaps in relation to the deployment, development and use of innovative technologies to fight fraud more effectively; c) identifying the actions needed to address such threats and vulnerabilities

Q.4.1 Are there any AI tools that you use as part of your national anti-fraud strategy or AFS to protect the financial interests of the Union?

Response	Frequency	Percentage	Member States
No	21	77.8%	AT, BE, BG, CY, DE, DK, EE, EL, FI, HR, IE, LT, LU, LV, MT, NL, PL, RO, SE, SI, SK
Yes, as part of other AFS	6	22.2%	BE, ES, FR, HU, IT, SI
Yes, as part of the NAFS	3	11.1%	CZ, IT, PT

Q.4.2 Please specify which AI tools you use as part of your NAFS?

Member State	Response
CZ	Automatic transcription and translation of wiretaps using AI: the main advantage of this is that speakers can be detected and identified and that natural language queries can be asked over the processed texts of wiretaps. We are also able to create automatically generated summaries of the text of wiretaps. The application is under development, with the focus on removing unwanted sounds in a recording, recognising foreign languages for better translation and extracting vital identities (of interest).
IT	The use of advanced technologies, including solutions based on artificial intelligence and machine learning, is part of the broader process of strengthening fraud prevention and detection systems promoted in particular by AGEA (Agricultural Payments Agency). In terms of planning and operations, AGEA has launched initiatives to modernise anti-fraud checks geared towards advanced data analysis and the detection of anomalous patterns, in line with developments in national and European anti-fraud strategies and the integrated use of risk analysis tools such as Arachne.

Member State	Response
PT	With a view to increasing the effectiveness, efficiency and proportionality of audits, the AI4Audit project (funded by the Technical Support Instrument) has developed AI-derived models to detect and predict irregularities in EU funds. This makes audits less work-intensive and more accurate.

Q.4.3 Please specify which AI tools you use as part of other AFS? Which AFS are they a part of?

Member State	Response
BE	FPS Finances (Customs disputes): SAS Enterprise Guide and Python – part of the risk management and selection strategy
ES	The Strategic Plan of the Tax Agency uses artificial intelligence tools to identify risky operations in the field of e-commerce, both at the time of clearance and for subsequent controls. The specific tools used are algorithms designed in-house by the Spanish Tax Agency.
FR	Given the ever-increasing level of sophistication and intensity of fraud involving public finances and the EU budget committed in cyberspace, it was deemed useful to organise effective cooperation between the State services responsible for combating fraud in cyberspace more specifically. The MICAF therefore intends to share maps of online fraud together with the most appropriate detection solutions (e.g. a benchmark for arrangements to analyse crypto-currency transactions). This flagship action is part of the new roadmap of the national anti-fraud strategy for the EU budget.
HU	In 2025 we carried out AI analyses using AI models and solutions developed by us. In order to protect tax secrecy and personal data, our solutions operated in a closed IT environment and, where necessary, on anonymised datasets. Preparatory work has been carried out on the applicability of a large commercial AI platform (LLM). We carried out AI developments for fraud detection under a National Tax and Customs Administration strategy (tax strategy, IT sub-strategy).
IT	Verification mechanisms using artificial intelligence have already been introduced in the fund management information system, SIF2127. Many processes are currently undergoing digital reprocessing, with artificial intelligence solutions also expected to be applied.
SI	Financial Administration of the Republic Slovenia: We use QlikSense (QS) portal as an IT analytic tool and self-developed applications for different areas of our responsibilities within QS for analytical work, risk analyses, risk management, and consequently for planning activities. AI, machine learning (ML), Insight Advisor and natural language processing (NLP) are integrated within QS. Within QS, the Insight Advisor leverages ML and NLP to understand users' questions, automatically analyse data, and generate visual insights that explain what is happening and why. Qlik Intelligence features further use NLP and generative AI to translate insights and predictions into clear, natural-language explanations, enabling users to easily understand results and make data-driven decisions directly within QS. These features are currently used in our analytical work to a limited extent.

Q.4.4 (AI users) What are the main uses of Artificial Intelligence within your systems?

Response	Frequency	Percentage	Member States
Anomaly detection	8	29.6%	BE, CZ, ES, FR, HU, IT, PT, SI
Predictive analytics	8	29.6%	BE, CZ, ES, HU, IT, PL, PT, SI
Automated classification	5	18.5%	BE, CZ, ES, HU, IT
Natural language processing	5	18.5%	BE, CZ, HU, LV, SI
Pattern recognition	4	14.8%	BE, CZ, HU, SI
Other (please specify)	5	18.5%	BE, EE, ES, IT, SK
None	17	63.0%	AT, BG, CY, CZ, DE, DK, EL, FI, HR, IE, LT, LU, LV, MT, NL, RO, SE

Please specify "Other" uses.

Member State	Response
BE	SPF Finances (Customs litigation): Network analysis
EE	We are currently in an exploratory phase with AI, but our organisations have already carried out a Copilot-related risk assessment and are able to use the tool in practice. This early stage allows us to test different use cases, evaluate benefits and limitations, and gradually integrate AI solutions in a controlled and responsible manner.
ES	An intermediate body uses AI to assist in the programming of computer applications.
IT	Law No 132 of 23 September 2025 – the first comprehensive national measure following the AI Act – laid down principles and delegating powers for the use of artificial intelligence that respect privacy, dignity, equality, security and transparency, harmonising national legislation with Regulation (EU) 2024/1689 and introducing monitoring mechanisms. With a view to combating fraud, the new offence of deepfakes (Article 612-quater of the Criminal Code) stands out. It punishes, with a term of imprisonment of one to five years, the dissemination of content that has been falsified or altered through the use of artificial intelligence systems that is likely to mislead. Other points of note include the generic

Member State	Response
	aggravating circumstance for offences committed by means of AI (Article 61(11-decies) of the Criminal Code), and the increase in penalties for financial offences, with special aggravating factors for circumventing and manipulating the market when carried out by means of AI systems. These safeguards are particularly relevant for preventing fraudulent conduct through the use of false identities, voice phishing, digital document manipulation and disinformation campaigns used for economic and financial offences. The Customs and Monopolies Agency is heavily involved in a programme to renew equipment aimed at adopting state-of-the-art non-intrusive verification technologies, including through the EU co-financing programme (CCEI) for customs controls and chemical laboratories. These innovative tools are designed to support the automatic detection of non-tax offences in the context of customs checks at certain airport customs offices located in the main postal and delivery service hubs which manage commercial traffic flows linked to e-commerce or those dedicated to checking the baggage of international passengers. Operations using AI/ML-based models for the identification of cigarettes, drugs, weapons, explosives, and undeclared currency are currently being developed. As regards the protection of the 'Made in Italy' brand and the fight against counterfeiting, the 'AUTENTICA' mobile application, currently at the initial trial operational phase, uses artificial intelligence and computer vision to assist officials during anti-fraud checks. The Ministry of Justice has continued to follow the plan outlined in the NRRP aimed at expanding the digitisation of files to cover those under the responsibility of both the civil (justices of the peace, juvenile courts, first and second instance proceedings on merits) and criminal (criminal sections of courts, courts of appeal and public prosecutor's offices) sectors. In parallel, the digital infrastructures for wiretapping were upgraded through the Digital Interception Database (Archivio Digitale delle Intercettazioni – ADI). In February 2025, the migration and synchronisation of content from the Public Prosecutor's Offices' local systems to the centralised inter-district systems was completed, with new interceptions delivered via that system in ISO format. Thus, the traceability of processes and the overall control of risk points have been strengthened, increasing transparency and accountability over the course of the entire lifecycle of judicial data. Another aspect is 'Datalake Giustizia', a NRRP project aimed at centralising the functions of extracting, querying and storing data on proceedings, with an interactive dashboard linked to criminal records (REGEWEB) and information fed into it by the court's Case Management System (SICP) and the Electronic Crime Reporting Portal (NdR). The tool, which will gradually be rolled out into more areas, enables constant monitoring of proceedings and key indicators (types of crime, population profiles, territorial distribution), which makes it possible to analyse phenomena in a timely manner, gauge the timing of urgent and precautionary measures, assess the impact of related civil proceedings and, above all, pre-emptively implement measures in vulnerable areas to prevent risk escalation. The integration of these elements (digitisation of files, inter-district interception systems, anti-fraud strategy with AI/ML safeguards and data lake analysis) has produced a single platform that combines interoperability, data quality and predictive capacity, providing administrations and judicial authorities with operational levers and information that adheres to European standards for the protection of the EU's financial interests.
SK	Automated checks of invoices

Q.4.5. Have you conducted a cyber/AI threat assessment in 2025?

Response	Frequency	Percentage	Member States
No assessment was conducted or planned	15	55.6%	BG, CY, DE, DK, EL, FI, FR,

Response	Frequency	Percentage	Member States
			HR, HU, LT, NL, PL, PT, RO, SI
Yes, a partial assessment was conducted	8	29.6%	AT, BE, EE, ES, IE, LV, MT, SK
Yes, a comprehensive assessment was conducted	3	11.1%	CZ, LU, SE
No, however we are planning/have planned an assessment	1	3.7%	IT

Q.4.6 What were the main findings of the threat assessment?

Member State	Response
AT	BMLUK (Federal Ministry for Agriculture): In 2025, cyber threats were systematically considered as part of the existing information security management system (ISMS) (risk analysis includes cyber threat scenarios). Dark web analyses are also performed to identify potential dangers at an early stage and continually improve information security. Technological developments, particularly in the area of artificial intelligence, are taken into account. In addition, there is a risk assessment by the paying agency Agrarmarkt Austria (AMA) on the topic of security and AI for that institution.
BE	Europa WSE (ESF Flanders): Europa WSE (ESF Flanders) is part of the Department WEWIS. The department has performed different Cyber/AI assessments in 2025, related to the security framework ISO27001, the NIS2 legislation, the CyFun framework of the CCB, the European AI Act, ... Last year's threat assessment concluded that there were no new major threats impacting our environment and no significant security incidents occurred. In addition, penetration tests identified zero critical or high vulnerabilities, confirming the overall strength of our security posture. There are some lower risk threats that are not mitigated on our roadmap. New critical software vulnerabilities are solved within the first weeks.
CZ	In the ongoing risk analysis, the most significant vulnerability discovered was an obsolete version of the Apache Tomcat application server. The results are not yet available. However, we note that the improvement of measures is fully dependent on the allocation of sufficient funds.
EE	Our public-sector employees are required to complete annual self-study training on cybersecurity and to pass a test at the required level. Regular training ensures that employees' knowledge and skills meet current security requirements and that they are able to prevent and identify potential threats. The training and testing are carried out within the designated training system, which ensures consistent content, monitoring, and compliance.

Member State	Response
ES	The responses from the various entities consulted cover the four possible answers. Among the positive responses are the following: The Spanish Tax Agency (AEAT) as a whole, through its Tax Information Technology Department, continuously analyses cyber threats, as does the General State Comptroller's Office (IGAE) through its Budget Information Technology Office, in order to establish security measures for the systems. One intermediary body indicates the following cyber threats detected in its information security policy: accidental or deliberate damage that may affect the availability, integrity or confidentiality of the information processed or the services provided; rapidly evolving threats with the potential to impact the confidentiality, integrity, availability, intended use and value of information and services. Other agencies indicate that they include a specific risk related to computer damage in their risk assessment matrix, with the result of the assessment being an acceptable risk, while another indicates that they identified new potential risks that they attempted to mitigate with the resulting action plan.
IE	The Department of Agriculture conducts this annually to achieve their ISO status. There were no major findings in 2025.
LU	The national IT (CTIE) performs these assessments on a regular basis.
LV	Internal regulation is needed for the use of AI in an institution. Determining the responsibility of the data regulation for the use of AI in an institution.
MT	The Ministry for European Funds and the Implementation of the Electoral Programme (MFI) remains a core participant in a centralised cyber threat assessment framework managed by the Malta Information Technology Agency (MITA). While the technical execution and primary data analysis are conducted at MITA level to ensure a unified 'Whole-of-Government' security posture, these assessments directly encompass all Ministry-specific systems such as emails. Consequently, the Ministry is continuously assessed against emerging threats, with security updates and mitigation strategies implemented as a direct result of MITA's ongoing findings. Access to the findings of these threat assessments is held within MITA.
SE	The authority noted the importance of supply chain security and has begun strengthening it.
SK	In the Slovak Republic, the obligation to assess cybersecurity risks for public sector entities, including cyber threats and threats related to artificial intelligence, is set out in national legislation (Act No. 69/2018 Coll. on Cybersecurity). The Government Office of the Slovak Republic (AFCOS) and Ministry of Investments, Regional Development and Informatization of the Slovak Republic conducted a risk assessment in 2025, which confirmed the need for continuous monitoring of cyber threats and threats related to artificial intelligence, implementation of appropriate preventive and organisational measures, as well as regular review and update of security controls in response to evolving risks. Given the sensitive nature of information related to cyber threats and threats related to artificial intelligence, detailed findings, namely vulnerabilities, tools used, and mitigation measures taken, are subject to limited access and cannot be shared beyond the scope required by applicable law.

DISCLAIMER ON ARACHNE

The Financial Regulation creates a legal basis for a modernised data-mining and risk-scoring tool, what we refer to as “Arachne+”, for the purposes of budget implementation. Overall, the objective of Arachne+ is to improve even further the efficiency of the tool and at the same time to reduce the administrative burden and provide a user-friendly tool to prevent, detect, correct, and follow-up on irregularities such as fraud, corruption, conflicts of interest, double funding.

As set by the Financial Regulation, Arachne+ will be applicable to all management modes, and the Member States will have an obligation to input data as from the post-2027 MFF (i.e. from 1 January 2028).

In terms of its use by the Member States, it will remain voluntary, however, in a joint statement on the occasion of the adoption of Regulation 2024/2509, there was a commitment by the Council, Commission, and Parliament to reassessing mandatory use of the tool for the post-2027 MFF, based on a Commission assessment of the tool's readiness by 2027.

The Expert Group was established by Commission Decision C(2024)7889 to formalise the cooperation between the Commission and the Member States towards the further development of the system and its generalised use by the Member States, and the development of the tool in consultation with its potential users. The work of the Expert Group will provide the Member States' input in the design of the tool and will be included in the assessment of readiness for the mandatory use of the tool by the Member States.

The Member States were invited to nominate their national representatives to the Expert Group at the end of 2024.

There are 4 main criteria to be targeted by the assessment of readiness, leading to potentially re-open discussions on mandatory use. These are aligned with the key objectives of the development of the future tool:

Risk indicators - shall be sufficiently uniform, objective, proportionate, necessary for risk assessment and based on reliable sources of information; Interoperability - interoperability with relevant IT systems and databases, including those of Member States, allowing for an automatic transfer of the relevant information in real time where feasible, and avoiding duplication of reporting; Artificial intelligence - for analysing and interpreting data; and in addition, Data protection – that the system shall comply with general data protection principles.

If you have any queries on the development of Arachne+ or would like to have further information

Q.4.7 What is your Arachne integration status?

Response	Frequency	Percentage	Member States
Partially feeding data into the system (minimum mandatory dataset)	15	55.6%	AT, CY, CZ, DK, EL, ES, FI, FR, HU, IE, LU, LV, MT, PL, SI
Feeding all possible data into the system	8	29.6%	BE, BG, EE, HR, IT, PT, RO, SK
No plan to adopt	2	7.4%	DE, LT
Planning to adopt	2	7.4%	NL, SE

Q.4.8 If you are only partially feeding data into Arachne, what are the reasons?

Response	Frequency	Percentage	Member States
Technical limitations	8	29.6%	CY, CZ, EL, ES, FR, IE, LU, SI
Strategic choice (only minimum dataset needed)	7	25.9%	CZ, ES, FI, FR, LU, LV, SI
Legal constraints	6	22.2%	AT, CY, ES, FR, PL, SI
Data not available in national systems	5	18.5%	CY, CZ, EL, FI, FR
Limited staff capacity	5	18.5%	CZ, ES, FI, FR, LU
Other (please specify)	8	29.6%	CZ, DK, ES, FI, HU, IE, MT, PL

Please specify "Other" reasons.

Member State	Response
CZ	The scope of the data and the frequency of updates was established at national level by the Ministry for Regional Development. The scope is set in the National Recovery Plan methodological environment.
DK	Arachne is not widely used in Denmark, so article 22 data from RRF is uploaded every 3rd month to Arachne.
ES	Responses regarding the Arachne integration status vary depending on the programme management authorities and even at the level of intermediate bodies within the same programme, covering the five possible answers to question Q.4.7.
FI	Implementation of the RRF will end at the end of 2026.
HU	Beyond the minimum dataset, we feed in the data laid down in Hungarian legislation in line with the commitment under the conditionality procedure.
IE	Bodies who are using Arachne are utilising it and feeding all possible data into the system. Some bodies are in the process of implementing it. This context led to the answer of partially feeding data.
MT	All minimum mandatory data is being transmitted to Arachne, together with any additional optional data that is currently available.
PL	Arachne is currently used as part of the National Recovery and Resilience Plan, including for the cyclical transmission of the input data. The institution sends this data, which is obligatory. In addition, it is necessary to streamline the process for inputting data in order to reduce administrative burdens. Legal barriers have also been identified, particularly as regards compliance with national data protection rules.

Q.4.9 For which funds is Arachne currently implemented?

Response	Frequency	Percentage	Member States
ERDF	17	63.0%	BE, BG, CY, CZ, ES, FR, HR, HU, IE, IT, LU, LV, MT, PT, RO, SI, SK
ESF / ESF+	17	63.0%	AT, BE, BG, CY, CZ, FR, HR, HU, IE, IT, LU, LV, MT, PT, RO, SI, SK
RRF	17	63.0%	BE, BG, CY, CZ, DK, EL, FI, HU, IE, IT, LV,

Response	Frequency	Percentage	Member States
			MT, PL, PT, RO, SI, SK
CAP – Pillar II (Rural Development)	12	44.4%	CY, EE, EL, ES, HR, HU, IT, LV, PT, RO, SI, SK
EMFAF	12	44.4%	BE, BG, CY, CZ, EE, ES, HR, HU, LV, PT, RO, SK
Cohesion Fund	11	40.7%	BE, BG, CY, CZ, HR, HU, LV, MT, PT, RO, SK
AMIF / ISF / BMVI	7	25.9%	BE, BG, CZ, HU, PT, RO, SK
CAP – Pillar I	6	22.2%	CY, EE, ES, IT, LV, PT
Other national or EU-funded programmes (please specify)	7	25.9%	AT, BE, HR, HU, IE, RO, SK

Please specify other national or EU-funded programmes.

Member State	Response
AT	JTF
BE	PSW ERDF Wallonia: BAR
HR	Contribution from the Ministry of Agriculture, Forestry and Fisheries, Directorate of Fisheries: Under the EMFAF, the Intermediate Body of the Managing authority has been delegated part of the selection of operations function. Namely, the IB performs checks on procurement procedures for beneficiaries who are not subject to public procurement obligations. In these procedures, the IB uses Arachne. The EMFAF Managing authority does not use Arachne. Contribution from the Ministry of Regional Development and EU funds: Fund for European Aid to the Most Deprived (FEAD) and Youth Employment Initiative (YEI)
HU	Brexit
IE	The Department of Agriculture are currently planning to adopt in respect of the CAP and EMFAF funds.

Member State	Response
	The Special EU Programming Body use Arachne for PEACEPLUS approved and contracted projects. Arachne is built into the EPPM that the Department of Justice uses for the AMIF fund. Work is continuing on this to ensure effective utilisation. BMVI and Cohesion Fund are not applicable to Ireland
RO	Just Transition Fund
SK	In addition to the listed funds, Arachne is implemented for the following additional programs: - CFP (Common Fisheries Policy): Arachne supports projects related to the management and funding of fisheries resources. - EU Solidarity Fund: Arachne assists in managing financial resources allocated for disaster relief and recovery. - Horizon Europe: While primarily a research and innovation fund, elements related to project management and compliance monitoring can benefit from Arachne's functionalities. - Just Transition Fund - Interreg VI-A Slovakia – Czech Republic 2021 – 2027

Q.4.10 How would you describe the level of implementation across these funds.

Response	Frequency	Percentage	Member States
Pilot phase for some funds	3	11.1%	ES, FI, SI
Implemented only for a limited number of funds	7	25.9%	DK, EE, EL, IE, LU, LV, PL
Implemented for most funds	8	29.6%	BE, BG, CY, FR, HR, MT, RO, SK
Fully implemented for all funds	5	18.5%	AT, CZ, HU, IT, PT

Q.4.11 Are there any AI tools you use that would benefit from accessing the data available in Arachne or that could improve Arachne's performance, adoption rate by national authorities or effectiveness?

Member State	Response
AT	No.
BE	PSW ERDF Wallonia: At the level of the Walloon Region, not for the moment ERDF and RRF Brussels Capital Region: No use made of AI tools by the ERDF and RRF Brussels Capital Region Europa WSE (ESF Flanders): We do not know of any AI tools as such. It would benefit us if Arachne would be more accessible/easier to interpret (with regards to action/follow-up). We do not currently use any AI tools. Communauté germanophone: No AI tools used
BG	Not yet
CY	N/A
CZ	None.
DK	We don't currently use AI-tools.
EE	We are not yet using AI tools that directly integrate with Arachne, but several types of solutions could benefit from access to its data. AI-based text analysis, pattern recognition and predictive models could improve anomaly detection and risk scoring. In the future, such tools could also support Arachne's performance and help increase its adoption once national implementation progresses and data access is ensured.
EL	No. AI tools are not used at this stage.
ES	No
FI	Not currently.
FR	The authorities managing cohesion policy funds which employ Arachne for their management and control system do not use tools with AI-based functionalities.
HR	Contribution from the Ministry of Labour, Pension System, Family and Social Policy: No. Contribution from the Ministry of Regional Development and EU funds: AI tools are not currently in use.
HU	No, there are no such tools at present. We recommend allowing such data to be transmitted to the Member States' monitoring and information systems in order to facilitate access to information and reduce the administrative burden.
IE	n/a
IT	Advanced data analytics and decision support tools, including those based on machine learning techniques, could significantly benefit from access to the data available in

Member State	Response
	Arachne. Further integration would improve the quality of risk analyses, improve the detection of anomalous patterns and reduce false positives, helping to increase the overall effectiveness of Arachne and facilitate its wider uptake by the competent national authorities.
LU	N/A
LV	No
MT	Currently the full use of AI is still being examined.
PL	There are tools at national level that would benefit from accessing the data available in Arachne because of the data it contains from other Member States sent by foreign institutions.
PT	No
RO	n/a
SI	NO
SK	At this time, some authorities use only a limited number of AI tools. These tools are mainly simple AI-based assistants built on large language models and are used for general support purposes only. They are not integrated with ARACHNE and do not currently require access to Arachne data, nor are they designed to improve ARACHNE's performance, adoption rate, or effectiveness.

Q.4.12 When using Arachne, what are the main challenges that you face?

Response	Frequency	Percentage	Member States
False alerts	19	70.4%	AT, BE, CY, CZ, DK, EE, EL, ES, FR, HR, HU, IT, LU, LV, MT, PL, PT, SI, SK
Difficulty interpreting indicators	18	66.7%	BE, BG, CZ, DK, EE, EL, ES, FI, FR, HR, HU, IE, IT, LV, PT, RO, SI, SK
Incompatibility issues (Filetype concerns, data quality, size limits)	14	51.9%	AT, BE, CZ, ES, FI, FR, HU, IE, IT, LU, PL, PT, SI, SK

Response	Frequency	Percentage	Member States
Legal concerns (e.g., Data Privacy)	11	40.7%	AT, BG, CZ, ES, FR, HU, IE, PL, RO, SI, SK
Other (please specify)	8	29.6%	CZ, EE, ES, FR, HR, MT, PL, RO

Please specify "Other" challenges.

Member State	Response
	The difficulty of ex-ante controls; missing time periods and data sources; impossibility of sanction monitoring; unclear audit trail of Arachne data; lack of information from national records of beneficial ownership.
CZ	Data insufficiently updated. Arachne does not yet include data from the Comenius operational programme and other operational programmes from the 2021-2027 programming period, so it has not been possible to make full use of Arachne. According to information from the working party for the 2021-2027 monitoring system there is a problem validating uploaded batches, which must be at least 95% validated to be uploaded to the production environment.
EE	Our PRIA has an internally developed risk system, so we have challenges to merge our system with Arachne.
ES	Legal validity of the results
FR	In order to calculate all the risk indicators in Arachne, data must be incorporated for which no provision for recording and collection is made in the sectoral regulations on funds. In the implementation of cohesion policy in France, users import into Arachne only data which are recorded and stored in the programme's data recording system. Some data recording systems are themselves connected with other databases which have APIs, such as those of INSEE (establishment data) and the INPI (beneficial owners). Feeding data into Arachne when it does not work in an interoperable or automated way with other databases becomes a technical and time-consuming exercise requiring operational support.
HR	Contribution from the Ministry of Labour, Pension System, Family and Social Policy: When checking potential conflict of interest for private persons there is no unique identification information (such as VAT number) that would help determine the identity of a person – in this way these checks seem useless.
MT	Identity Card or Passport Numbers cannot be inserted in the system.
PL	Some flaws in the functionalities of the tool and difficulties in using it have been 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 burdens related to the collection of data for, unclear algorithms for the calculation of individual risk indicators and no service desk tool to deal with errors. Problems have also been identified with downloading large data packages in a single session and slow response times when processing larger amounts of data.

Member State	Response
RO	There is no possibility for automated data extraction and integration into the Arachne file. The Ministry of Energy compiles an Excel file manually, using data from the proiecte.pnrr.gov platform and the Contract Monitoring unit, without any degree of automation. For such automation to be feasible, the Ministry of Energy would need access to the Arachne platform and trained staff capable of exporting data from Excel files to the Arachne platform. Ministry of Investments and European Projects: SMIS Audit Authority: Difficulties in exporting data from the national management systems (e.g. SMIS 2021+, eMS) to Arachne.

Q.4.13 Has Arachne been incorporated into your NAFS or other AFS?

Response	Frequency	Percentage	Member States
Yes, as part of the NAFS	10	37.0%	BG, CY, CZ, DK, HU, IT, MT, PT, RO, SK
Yes, as part of other AFS	9	33.3%	AT, BE, CY, EE, EL, IE, IT, LU, SI
No, but implementation is being considered	4	14.8%	ES, FI, FR, PL
No	3	11.1%	ES, HR, LV

Q.4.14 Are your data analysis tools interacting with Arachne?

Response	Frequency	Percentage	Member States
No	10	37.0%	BE, CY, DK, EL, ES, FI, FR, HR, LV, PL
Yes (please specify which)	6	22.2%	AT, CZ, IT, MT, RO, SK
Not yet, but planned (please specify which)	5	18.5%	BG, EE, LU, PT, SI

Response	Frequency	Percentage	Member States
Not applicable	2	7.4%	HU, IE

Q.4.15 Please list the data analysis tools which are/are planned to interact with Arachne.

Member State	Response
AT	Databank: IDEA.
BG	It is planned to adapt and synchronised analysis tools with ARACHNE
CZ	Arachne is used as the basis for risk analyses for planning on-the-spot checks.
EE	Internal risk scoring system
IT	‘Among the data analytics tools planned to interact with Arachne is the “SAS (Statistical Analysis System) platform”, which is used for advanced data analytics and to support fraud detection and prevention activities. The inclusion of SAS is consistent with AGEA Circular No 34322 of 28 April 2025 and is part of the broader strengthening of the risk analysis and decision-making support systems available to the relevant authorities. The Inspectorate-General for Financial Relations with the European Union (IGRUE) of the Ministry of Economic Affairs and Finance (MEF) has continued to participate in the Arachne expert group set up by European Commission Decision of 20 November 2024 (C(2024) 7889 final), aimed at designing a corporate data mining and risk scoring tool to prevent, detect, correct and monitor irregularities, including fraud, corruption, conflicts of interest and double funding. IGRUE appointed one of the members representing Italy and has begun discussions with the national working group with a view to sharing the Italian position to be put before European experts on the diverse issues discussed at the various planned meetings’.
LU	Our own data exchange platform cannot interact with Arachne (no upload currently possible). It is foreseen to have this for 2028-2034.
MT	The data analysis tool interacting with Arachne is the Management and Control Information System (MCIS), formerly the Structural Funds Database (SFD). MCIS is Malta’s central system for the management, monitoring, and payment processing of EU-funded operations. When Arachne identifies risk indicators or red flags, the outputs are further analysed within MCIS using detailed project, financial, and beneficiary data to support any follow-up checks.
PT	The plan is to ensure that Arachne will be interoperable with the IT systems of the European Funds.
RO	Ministry of Energy: Operational procedures for the management of irregularities, anti-fraud and anti-corruption policy, checklists and questionnaires on the identification of serious irregularities and fraud indicators.
SI	-
SK	Information and monitoring system ITMS2014+ a ITMS21+. Regarding plans it’s currently difficult to confirm the tool as there were few discussions mentioning different information

Member State	Response
	system for next programming period. Some authorities use basic AI-assisted or spreadsheet-based tools for internal data handling, but these tools do not interact with Arachne. In the future, integration of additional data analytics tools may be considered, depending on legal requirements, data protection, and technical feasibility.

Q.4.16 How would you rate the interoperability of the systems on average?

Response	Frequency	Percentage	Member States
3 Medium Interoperability	3	11.1%	MT, RO, SK
4 High Interoperability	2	7.4%	AT, IT
1 Very Low Interoperability	1	3.7%	CZ

Q.4.17 Please explain the interaction of the two (or more) systems in your administration.

Member State	Response
AT	The data from the IDEA database is fed into Arachne via manual data upload. Information should be downloaded automatically from the MS2014+ system to Arachne. Data for the programming period 2021 onwards are not yet available in Arachne.
CZ	Our publicly available data analysis tools are not directly linked to the Arachne system. As for screening the risks and inspections of entities, we use supplementary systems such as ESM, EU Sanctions and other available databases that enable us to carry out more comprehensive verifications than would be possible using only the Arachne system. Accordingly, Arachne is one of the supporting sources of information rather than being the main (interconnected) analytical tool.
IT	The SAS platform developed by AGEA processes EU and national data collected in Arachne to produce more detailed and refined outputs, which are used to steer fraud prevention and detection activities, as well as for on-going risk monitoring. This interaction between Arachne and SAS, although not yet fully operational at all stages, is a key element of the anti-fraud data analysis ecosystem and a step towards broader interoperability between anti-fraud information management systems.
MT	Data is extracted from MCIS and uploaded in Arachne.
RO	Ministry of Energy: Automated data transfers from the NRRP platform to Arachne are not possible. Ministry of Investments and European Projects: Data retrievals from SMIS for insertion into Arachne.

Member State	Response
	Regional Development Agency: Arachne interacts with the SMIS 2021 management IT system.
SK	Slovakia currently provide data only via XML export from national systems/import to Arachne. Discussions with the Arachne support team regarding automation of data exchange (API integration) are ongoing.

Q.4.18 Are you satisfied with the type of support available on Arachne?

Response	Frequency	Percentage	Member States
Yes	9	33.3%	AT, CY, EE, FI, IE, IT, LV, MT, PT
No	9	33.3%	BE, BG, CZ, FR, HR, HU, RO, SI, SK
Not applicable/ We were not aware of such support	5	18.5%	DK, EL, ES, LU, PL

Q.4.19 What type of support (training/content/guidebooks) on Arachne would be the most useful to you?

Response	Frequency	Percentage	Member States
Training for staff (from induction training to expert training)	13	48.1%	BE, BG, CZ, EL, ES, FR, HR, HU, LU, PL, RO, SI, SK
Arachne Academy tutorials/videos	12	44.4%	BE, BG, CZ, EL, ES, HR, HU, LU, PL, RO, SI, SK
Guidance on risk indicators and their interpretation	12	44.4%	BE, BG, CZ, EL, ES, FR, HR, HU, LU, RO, SI, SK

Response	Frequency	Percentage	Member States
Technical assistance	10	37.0%	BE, CZ, EL, ES, HR, HU, LU, PL, RO, SI
Arachne forum (peer exchange)	8	29.6%	BE, CZ, EL, ES, HR, HU, RO, SI
Financial support	4	14.8%	CZ, ES, HR, HU
Other (please specify)	2	7.4%	DK, FR

Please specify "Other" type of support.

Member State	Response
DK	.
FR	For assistance with cohesion policy, users currently rely on the expertise of their correspondent in the European Commission in order to import data in the expected format. The Commission also offers some training sessions for users. However, it would probably also be necessary to develop tailored assistance to improve the programme information systems so that they are fully compatible with Arachne. Furthermore, users often also request assistance to interpret the risks identified by Arachne.

Q.4.20 How do you plan to (further) incorporate digitalisation into your (future) national anti-fraud strategies?

Member State	Response
AT	Not yet decided.
BE	Belgian AFCOS: The ambition is to fully integrate digitalisation in our anti-fraud strategies. Europa WSE (ESF Flanders): At Europa WSE, we are currently in the process of implementing CATE, an AI program that will help our checks during the reporting.
BG	Not applicable yet
CY	We plan to implement the NAFS digitalisation actions: establish a working group to map data sources and tools (including AI applications), conduct a systems/databases mapping exercise, develop a concept for a data integration tool in consultation with relevant

Member State	Response
	stakeholders, explore funding options, and ensure fuller utilisation of Arachne, including systematic upload of programme and transaction data.
CZ	With the development and introduction of relevant tools and processes in the state administration, further updates of the NAFS will comprise their use for the anti-fraud area.
DE	Further integration will be considered after checking compatibility with existing IT systems and the legal situation.
DK	Danish Business Authority: In the new programming period we plan to use Arachne+. Danish Agricultural and Fisheries Agency: At the moment, adoption of Arachne is the primary focus of future digitalization of our anti-fraud efforts.
EE	We plan to further integrate digitalisation into our national anti-fraud strategies by expanding the use of data-driven tools, improving access to interoperable information systems, and strengthening analytical capabilities. This includes continuing to experiment with the use of artificial intelligence—such as text analysis and pattern recognition—in areas where it can increase the effectiveness of controls. We also intend to assess opportunities to safely implement and use AI-based tools in risk analysis and to identify patterns through enhanced data analytics. To mitigate fraud risks, different digital elements, including AI-based solutions, should be embedded at every stage of application processing to ensure timely prevention or detection of irregularities. As national discussions progress and as tools like Arachne+ become more fully implemented, our approach will be further refined. We also closely monitor developments and best practices in other countries, which inform and guide our digitalisation decisions.
EL	Article 50(1) of Law 4914/2022 provides for the digitalisation of the handling (receipt and examination) of complaints concerning programmes/projects co-financed under the ESPA. This should be implemented in the Integrated Information System within the year.
ES	Improvement of tools for risk analysis, the widespread use of databases for prevention and detection purposes, and the analysis of the interoperability of databases. According to a management authority consulted, incorporating data from its management application files into Arachne, in compliance with European regulations. Establishment of digital platforms for transparency and oversight, big data analysis systems, and the use of AI to identify anomalies and predict corruption risks. In updates or new general or specific management risk prevention plans. Use of AI to facilitate preliminary analysis of complaints received.
FI	Making use of Arachne and other officially recorded data.
FR	Under consideration
HR	Not applicable.
HU	We are working continuously on the digitalisation of fraud prevention and detection processes and tools.

Member State	Response
IE	The authorities in Ireland have stressed the importance of digitalisation and digital tools in anti-fraud efforts.
IT	Digitisation will be further incorporated through enhanced interoperability between information systems, the use of advanced data analytics and decision support tools, as well as the progressive use of technological solutions geared towards risk analysis and fraud prevention. Particular attention will be paid to integration between databases, data quality and training of the staff involved.
LT	-
LU	N/A
LV	Possibilities of further digitalization will be analysed during elaboration of the next NAFS.
MT	The incorporation of digitalization will be considered at the time the NAFCS is updated.
NL	We will ensure that the systems operate firstly in accordance with privacy laws, then preferably in a coordinated manner with good instructions and regular refresher training.
PL	Poland has not adopted a national anti-fraud strategy (NAFS). There are no plans to draw up such a document at national level. IT tools are used in the anti-fraud process, for example during checks and verifications, when tracing networks of connections and checking conflicts of interest, and so on.
PT	The NAFS has measures in place covering digitalisation and the interoperability of IT systems.
RO	Through continuous and specialised training and investment in AI tools at the Ministry of Energy.
SE	There is no national strategy.
SI	Re Q4.7 The AKTRP has selected two means: Partially feeding data into the system... and Testing adaptability...
SK	Digitalisation will be introduced gradually, in line with the strategic objectives of the National Strategy for the Protection of the EU's Financial Interests in the Slovak Republic, with a focus on the systematic use of existing digital tools, such as the ARACHNE system, improving the quality and availability of data and increasing the awareness and capacities of national authorities. The current National Strategy for the Protection of the EU's Financial Interests in the Slovak Republic already defines a permanent task to ensure the implementation of sophisticated analytical software tools, including the ARACHNE system, in project evaluation and risk identification. The upcoming update of the National Strategy emphasises that digitalisation should be one of the key pillars of the protection of the European Union's financial interests in the Slovak Republic, across the entire anti-fraud cycle.

Q.4.21 Please select three barriers to the digitalisation of your anti-fraud efforts, that you believe are most crucial to overcome.

Response	Frequency	Percentage	Member States
Interoperability challenges	19	70.4%	CY, DE, EE, EL, ES, FI, FR, HR, HU, IE, IT, LU, LV, MT, NL, PT, SE, SI, SK
Budget constraints	16	59.3%	BE, BG, CZ, DK, EE, ES, FI, HR, HU, IE, LT, LU, LV, PL, RO, SK
Data protection concerns	12	44.4%	AT, BE, DE, EL, FR, HU, IE, LU, MT, PL, PT, SE
Legal issues	12	44.4%	AT, BG, CY, CZ, DE, EE, FR, LT, PL, RO, SE, SK
Skill gaps	10	37.0%	BE, DK, EL, FI, HR, IT, MT, PT, RO, SI
Outdated legacy systems	9	33.3%	BG, CY, CZ, DK, ES, IT, LT, LV, NL

Q.4.22 Please feel free to specify any other additional challenges or experiences regarding this section, which you would like to share.

Member State	Response
DE	The AMIF managing authority: The strict data protection requirements, the fact that there are different IT systems for each fund type and the lack of staff with adequate Arachne+ and IT skills also make using ARACHNE+ challenging. Additional answers to Q. 4.7 from individual managing authorities (multiple answers not possible): – Testing adaptability with national systems: The AMIF managing authority; The Lower Saxony ERDF managing authority

Member State	Response
	– Planning to adopt: The Brandenburg ERDF managing authority
EE	One of the key challenges we continue to face in the digitalisation of our anti-fraud efforts is ensuring consistent access to high-quality, interoperable data across institutions. Limited data availability or fragmented systems can slow down the effective use of digital tools, including risk-analysis platforms and AI-based solutions. Another important aspect is the human factor. Even when digital tools are available, the data is ultimately used and interpreted by people, and human errors can lead to incorrect assessments or create additional risks. Ensuring that staff have the necessary skills, training, and support to use these tools effectively is therefore essential. We also recognise the need to implement new technologies safely and responsibly. While digital tools offer significant potential, their integration requires careful consideration of data protection, security, and governance. Digitalisation efforts also progress at different speeds across organisations, which can create uneven capabilities and require additional coordination. We continue to monitor developments and best practices in other Member States, which help inform our decisions and guide our digitalisation efforts
EL	-
ES	Very rigid management applications, which make any change costly and time-consuming. Shortage of specialised human resources for the implementation of tools, processes, and procedures for the development of solutions for the digitization of the anti-fraud system and cooperation with external authorities.
HR	Contribution of the Ministry of Agriculture, Forestry and Fisheries (Paying Agency for Agriculture, Fisheries and Rural Development): Our future goal will be better use of IT, in particular data integration from different central base in order to lower administrative burden and to ensure the most efficient and effective use of EU fund.
IE	In respect of question 4.18. Satisfaction with support exists but increased supports welcome, i.e. EU or national level. Shared management members of AFCOS network will be discussing Arachne usage as a rolling agenda item going forward in order to facilitate conversations on best practice, key challenges and peer exchange etc.
NL	No further comments.
SI	in addition, regarding Q4.16: 2 Low interoperability

Q.5.1 Please list the national services and bodies consulted to reply to this questionnaire.

Member State	Response
AT	Federal Ministry of Agriculture and Forestry, Climate and Environmental Protection, Regions and Water Management. Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection. Federal Ministry of Finance.

Member State	Response
BE	FPS Economy - CICF (Interdepartmental Committee for Coordinating the Fight against Economic Fraud) - AFCOS BE
	FPS FINANCES
	FPS BOSA (Policy and Support)
	FPS JUSTICE
	COMMUNITIES (German-speaking, Flemish and French)
	REGIONS (Brussels Capital, Flemish and Walloon)
	ERDF, RRF & ESF BRUSSELS-CAPITAL REGION
	ERDF, RRF & ESF WALLONIA
	ERDF, RRF & ESF FLANDERS
	WALLOON PAYING AGENCY (ORGANISME PAYEUR WALLON (OPW))
BG	FLEMISH AGENCY FOR AGRICULTURE AND FISHERIES (AGENTSCHAP LANDBOUW & ZEEVISSERIJ)
	FEDERAL POLICE
	The Prosecution of the Republic of Bulgaria, Managing authorities, the National Fund Directorate within the Ministry of Finance (Certifying Authority/Accounting Body/Coordination Body at national level regarding the Recovery and Resilience Facility), the Central Coordination Unit within the Council of Ministers (central coordinator of the European Commission's SFC 2007 and SFC 2014 fund management systems at national level and of the Arachne), the AFCOS Directorate
	AFCOS Secretariat, Managing Authorities, Audit Office of the Republic, COPA, Cyprus Police, Management Authority, Tax Authorities and Customs Department.
	National Coordination Authority, Managing authorities, Component owners, Police of the Czech Republic - National organised Crime Agency, Prosecutor General's Office, General Customs Directorate.
	AFCOS Germany, the Federal Ministry of Finance, The Federal Foreign Office, The Federal Ministry of Labour and Social Affairs, The Federal Ministry of Agriculture, Food and Regional Identity, The Federal Ministry of Economic Affairs and Energy, The Federal Ministry of the Interior, The managing authorities of the federal states, Investitionsbank Schleswig-Holstein
	Audit Authority of the Danish Ministry of Finance
	Danish Ministry of Justice
	Danish Director of Public Prosecutions
	Danish National Special Crime Unit
DK	Danish Ministry of Taxation
	Danish Tax Agency
	Danish Customs Agency
	Danish Business Authority
	Danish Agency for Green Transition and Aquatic Environment
	Danish Agricultural and Fisheries Agency

Member State	Response
EE	The questionnaire was sent to 11 national bodies, and we received substantive input from eight of them.
EL	Εθνική Αρχή Διαφάνειας (ΕΑΔ) (National Transparency Authority) Επιτροπή Δημοσιονομικού Ελέγχου (ΕΔΕΛ) (Financial Audit Committee) Ειδική Υπηρεσία Θεσμικής Υποστήριξης & Πληροφοριακών Συστημάτων (ΕΥΘΥΠΣ) (Special Service for Institutional Support & Information Systems) Ειδική Υπηρεσία Συντονισμού Ταμείου Ανάκαμψης (ΕΥΣΤΑ) (Recovery and Resilience Facility Special Coordination Service) Υπουργείο Αγροτικής Ανάπτυξης και Τροφίμων (ΥΠΑΑΤ) (Ministry of Rural Development and Food)
ES	European Social Fund Administration Unit (UAFSE) Sub-Directorate General Economic Management and European Funds (managing authority for AMIF) Sub-Directorate General Economic Sustainability and Social Affairs (managing authority for European Maritime, Fisheries and Aquaculture Fund) Sub-Directorate General Inspection and Control (Directorate-General for European Funds) Sub-Directorate General European Territorial Cooperation (managing authority for ETC programmes) Sub-Directorate General Agricultural Funds- FEAGA (Spanish Agricultural Guarantee Fund - coordinating body of the paying agencies) FEAGA Internal Audit Division Sub-Directorate General ERDF (managing authority for ERDF) Sub-Directorate General Planning and Management of Infrastructures and Resources for Security (managing authority for ISF)) 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) State Agency for Tax Administration (AEAT)- Customs and Excise Department State Agency for Tax Administration (AEAT)- Department of Financial and Tax Inspection. Undersecretariat of the Ministry of Agriculture, Fisheries and Food -Anti-fraud and Internal Control Unit Civil Guard National Police
FI	Ministry of Finance, Ministry of Economic Affairs and Employment, Ministry of Agriculture and Forestry, Ministry of the Interior, State Treasury, Finnish Food Authority
FR	ANCT, MICAF, ANAFE, DGTrésor
HR	1. Ministry of Agriculture, Forestry and Fisheries and Paying Agency for Agriculture, Fisheries and Rural Development 2. Ministry of Justice, Public Administration and Digital Transformation 3. Ministry of Labour, Pension System, Family and Social Policy (Managing Authority for the Operational Programme Efficient Human Resources 2014-2020 and Programme Efficient Human Resources 2021-2027) and Intermediate body level 2 - Croatian Employment Office, Office for Financing and Contracting of EU Projects 4. Ministry of Regional Development and EU funds (Managing Authority for the Operational Programme Competitiveness and Cohesion 2014-2020 and Programme Competitiveness and Cohesion 2021-2027 and Integrated Territorial Programme) and Intermediate Bodies

Member State	Response
	level 2 - Central Finance and Contracting Agency for European Union Programmes and projects (CFCA), Croatian Agency for SMEs, Innovation and Investments (HAMAG-BICRO), Croatian Waters 5. Ministry of Finance, Customs Administration 6. Ministry of Finance, Tax Administration 7. Ministry of Agriculture, Forestry and Fisheries, Directorate of Fisheries - the EMFAF Managing Authority 8. Croatian AFCOS Unit at the Ministry of Finance
HU	The National Development Centre's Internal Audit and Integrity Directorate and Common Services Directorate, and the members of the Artificial Intelligence Working Group and the Irregularity Reporting Working Group. An Garda Siochana Department of Agriculture, Food and the Marine. Department of Education Department of Finance (AFCOS) Department of Further and Higher Education Department of Justice Department of Public Expenditure
IE	Department of Housing Department of Transport Garda National Economic Crime Bureau Special EU Programming Body Northern and Western Regional Assembly Southern Regional Assembly Eastern and Midland Regional Assembly Revenue Commissioners
IT	This follow-up was prepared with the involvement of all of the following institutions/administrations that make up the Italian AFCOS pursuant to Article 3 of Presidential Decree No 91/2007 and Article 3 of Decree-Law No 19/2024: Department for European Affairs at the Prime Minister's Office; Department for Cohesion Policy and Southern Italy at the Prime Minister's Office; Department of Public Administration at the Prime Minister's Office; Department for Regional Affairs and Autonomies at the Prime Minister's Office; NRRP Unit at the Prime Minister's Office; Special Economic Zones (SEZ) Unit at the Prime Minister's Office; Italian Court of Auditors;

Member State	Response
	Network of NRRP Anti-Fraud Contact Persons at the State General Accounting Department; Coordination Committee for High-Level Oversight of Priority Infrastructure and Construction Projects (CCASIIP); Carabinieri; the Guardia di Finanza (financial police); National Anti-Corruption Authority (ANAC); Financial Intelligence Unit (FIU) at the Bank of Italy; National Anti-Mafia and Anti-Terrorism Directorate; Central Criminal Police Directorate; Anti-Mafia Investigation Directorate; Ministry of the Interior; Ministry of Justice; Ministry of Economic Affairs and Finance; Ministry of Enterprises and Made in Italy; Ministry of Agriculture, Food Sovereignty and Forestry; Ministry of Infrastructure and Transport; Ministry of Labour and Social Policy; Ministry of Education and Merit; Customs and Monopolies Agency; Revenue Agency; Agricultural Payments Agency (AGEA); Joint Conference.
LT	Ministry of Finance, Ministry of the interior.
LU	Ministry of Housing and Spatial Planning - Ministry of the Economy - Ministry of Labour - Ministry of Agriculture, Food and Viticulture - Ministry of Finance and Ministry of Home Affairs
LV	All authorities from the AFCOS network.
MT	Ministry for European Funds and the Implementation of the Electoral Programme (MFI)
NL	Ministry of Justice, Ministry of Social Affairs, Ministry of Economic Affairs, Ministry of Agriculture (management authorities / policy implementation), paying agencies and AFCOS.
PL	Ministry of Funds and Regional Policy (partnership agreement coordinating authority), Agency for Restructuring and Development of Agriculture (paying agency) and Ministry of Finance (AFCOS).
PT	Inspeção-Geral de Finanças (inspectorate-general of finances) (AFCOS) Agência para o Desenvolvimento & Coesão (agency for development and cohesion) Instituto de Financiamento da Agricultura e Pescas (Institute for the funding of farming and fisheries) Estrutura de Missão Recuperar Portugal ('Portugal recovery' task force) Autoridade Tributária e Aduaneira (tax and customs authority)
RO	Romanian English translation Agência Națională pentru Achiziții Publice National Agency for Public Procurement Agência Națională de Administrare a Bunurilor Indisponibilizate National Agency for the Administration of Seized Assets

Member State	Response
	Agenția Națională de Administrare Fiscală National Agency for Fiscal Administration Agenția pentru Finanțarea Investițiilor Rurale Agency for the Financing of Rural Investments Agenția Națională a Funcționarilor Publici National Agency of Civil Servants Agenția Națională de Integritate National Integrity Agency Agenția de Plăți și Intervenție pentru Agricultură Agency for Payments and Intervention for Agriculture Autoritatea de Certificare și Plată Certifying and Paying Authority Consiliul Concurenței Competition Council Ministerul Afacerilor Interne Ministry of Internal Affairs Ministerul Agriculturii și Dezvoltării Rurale Ministry of Agriculture and Rural Development Ministerul Economiei, Digitalizării, Antreprenorialului și Turismului Ministry of Economy, Digitalisation, Entrepreneurship and Tourism Ministerul Culturii Ministry of Culture Ministerul Dezvoltării, Lucrărilor Publice și Administrației Ministry of Development, Public Works and Administration Ministerul Educației și Cercetării Ministry of Education and Research Ministerul Energiei Ministry of Energy Ministerul Muncii, Familiei, Tineretului și Solidarității Sociale Ministry of Labour, Family, Youth and Social Solidarity Ministerul Finanțelor Ministry of Finance Ministerul Investițiilor și Proiectelor Europene Ministry of Investments and European Projects Ministerul Mediului, Apelor și Pădurilor Ministry of Environment, Waters and Forests Ministerul Sănătății Ministry of Health Ministerul Transporturilor și Infrastructurii Ministry of Transport and Infrastructure Oficiul Național de Prevenire și Combateră a Spălării Banilor National Office for the Prevention and Control of Money Laundering Secretariatul General al Guvernului Secretariat-General of the Government Autoritatea Națională pentru Administrare și Reglementare în Comunicații National Authority for Management and Regulation in Communications Agenția pentru Dezvoltare Regională Nord-Est North-East Regional Development Agency Agenția pentru Dezvoltare Regională Sud-Est South-East Regional Development Agency Agenția pentru Dezvoltare Regională Sud Muntenia South-Muntenia Regional Development Agency Agenția pentru Dezvoltare Regională Vest – ADR Vest West Regional Development Agency (ADR Vest) Agenția pentru Dezvoltare Regională Sud-Vest Oltenia South-West Oltenia Regional Development Agency Agenția pentru Dezvoltare Regională București-Ilfov Bucharest-Ilfov Regional Development Agency Agenția pentru Dezvoltare Regională Nord-Vest North-West Regional Development Agency Agenția pentru Dezvoltare Regională Centru – ADR Centru Centre Regional Development Agency (ADR Centre) Parchetul de pe lângă Înalta Curte de Casație și Justiție Public Prosecutor's Office attached to the High Court of Cassation and Justice Autoritatea de Audit Audit Authority Autoritatea Vamală Română Romanian Customs Authority Ministerul Justiției Ministry of Justice
SE	The Swedish Agency for Economic and Regional Growth, the Swedish ESF Council and the Swedish Economic Crime Authority.

Member State	Response
SI	URSOO, AKTRP, FURS, UPPD, MNZ, MKRR.
SK	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 Informatization of the Slovak Republic, Ministry of Agriculture and Rural Development of the Slovak Republic, Agricultural Paying Agency, 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, Ministry of Education, Research, Development and Youth of the Slovak Republic, National Implementation and Coordination Authority (NICA)– Office of the Deputy Prime Minister of the Slovak Republic for the Recovery and Resilience Plan and Knowledge Economy.