EUROPEAN
COMMISSION

Brussels, 25.7.2024
SWD(2024) 190 final

COMMISSION STAFF WORKING DOCUMENT

Follow-up by Member States to the recommendations of the PIF Report 2022

Accompanying the document

Report from the Commission to the Council and the European Parliament

35th Annual Report on the protection of the European Union's financial interests and the fight against fraud - 2023

{COM(2024) 318 final} - {SWD(2024) 187 final} - {SWD(2024) 188 final} - {SWD(2024) 189 final} - {SWD(2024) 191 final} - {SWD(2024) 192 final} - {SWD(2024) 193 final}

Contents

List of abbreviations

AFCOS	Anti-Fraud Coordination Service
AFIS	Anti-Fraud Information System
CA	Certifying authority
CAP	Common agricultural policy
EPPO	European Public Prosecutor's Office
ERDF	European Regional Development Fund
ESIF	European Structural Investment Funds
ESF	European Social Fund
EU	European Union
IB	Intermediate body
IMS	Irregularity management system
MA	Managing authority
MCS	Management and control system
MFF	Multiannual Financial Framework
NAFS	National anti-fraud strategy
NRA	National risk assessment
OLAF	European Anti-Fraud Office
PIF	Protection of the EU's financial interests
RRF	Recovery and Resilience Facility
RRP	Recovery and resilience plan

Introduction

In its 2022 Report on the Protection of the EU's Financial Interests, the Commission made recommendations to Member States on: a) improving the detection, reporting and follow-up of suspected fraud; b) putting the digitalisation of the fight against fraud high on Member States' agenda; c) strengthening anti-fraud governance in the Member States.

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

1. Overview of Member States' replies to the questionnaire

1.1. *Recommendation 1: improving detection, reporting and follow-up of suspected fraud*

In the Member States with low incidence of fraud, the competent authorities should invest in fraud risk analysis in order to assess the degree to which low detection is the result of low levels of actual fraud affecting their operations or the result of systemic weaknesses in detection or reporting systems.

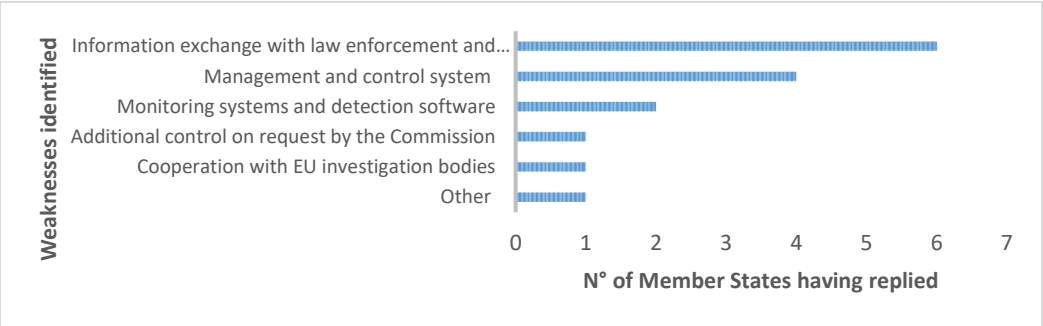
Member States should focus on detecting signals of fraud and, where irregularities are found, carefully addressing the question of intentionality.

If the identified issues point to reporting practices (e.g. Delaying classification as suspected fraud) Member States should review them also taking into account the need for a better information flow to and from judicial authorities.

1.1.1. Fraud risk analysis

Most Member States[1] assessed the incidence of fraud in their country as low.

Several Member States[2] indicated that they had conducted a fraud risk analysis to assess the reasons for low detection of suspected fraud in their operations. Half of those identified weaknesses in fraud detection. Such weaknesses mostly relate to 'information exchange with law enforcement and specialised agencies', as shown in the overview below.



It is hard to determine whether low levels of reported fraud are the result of specific anti-fraud measures. It is crucial that Member States continue to monitor fraud, while developing measures and tools to prevent it.

1.1.2. Instruments / core principles

Member States link success in preventing fraud to a a multi-stakeholder and multi-level approach that facilitates cooperation between all the relevant players, from national customs authorities to supranational institutions, as well as authorities in non-EU countries. They identify some key principles for cooperation, outlined below. :

[1] AT, BE (Wallonia), BG, CZ, DE, DK, EL, ES, FI, HR, HU, IE, LV, LT, MT, NL, PT, SK.

[2] AT, BE, BG, CZ, DE, EL, ES, FI, HR, HU, LV, LT, MT, NL, PT, SI

.

- Responsibilities between audit and control bodies within the Member States should be clearly distributed.
- Administrative and on-the-spot checks should take place regularly to keep the levels of incidence of fraud low.
- Data should be regularly sent to the Commission/European Anti-Fraud Office (OLAF) (via the IMS), to the European Public Prosecutor's Office (EPPO) and to national audit and control bodies in the Member State to help them keep track of pressing matters. These comparative data can then be used to assess the level of incidence of fraud.
- Some Member States[3] reported positive results from initiatives that facilitate the sharing of knowledge and best practices and that allow benchmarking the performance of Member States, while acknowledging variation in size, background, etc.
- All stakeholders recognised the importance of investing in:
    - training courses
    - compiling guidelines and
    - organising workshops, to keep the performance and quality of performance high.
- All institutions should use internal mechanisms, such as the four-eyes principle, to prevent fraud.

1.1.3. Intentionality

The intentionality of an irregularity is investigated as part of criminal prosecution, involving law enforcement agencies and public prosecutors. However, various Member States[4] acknowledged having other types of proceedings to assess intentionality, for example to decide about penalties. These include both criminal and administrative proceedings, such as tax inspection and checks to detect alterations to documents.

Adequate access to information is needed to assess whether the bodies in charge of detecting irregularities are able to detect intentionality. In the survey, nearly all Member States[5] declared that those bodies have adequate access to information to assess the possibility of intentionality.

Useful ways to assess whether an irregularity might be intentional and thus constitute a suspected fraud for the competent authorities to investigate further, include:

- using the risk-scoring tool ARACHNE;
- performing case-by-case analysis;
- analysing shortcomings in implementation;
- Injecting data and analysing risk indicators;
- examining links between the players involved, e.g. beneficiaries, contractors, subcontractors and suppliers;
- examining the legality of conditions for allocating public funds;
- examining the possible manipulation or falsification of documents.

[3] EE, EL, IT.

[4] CZ, EE, EL, ES, HR, HU, LV, PL, SI, SK.

[5] BE, BG, CY, CZ, DE, DK, EL ES, FI, FR, HR, HU, IE, IT, LT, LU, MT, NL, PL, PT, RO, SI, SK.

Member States also highlighted the importance of training to raise staff awareness of certain signs of possible cases of suspected fraud and of having more experienced staff share their knowledge and expertise with their colleagues and provide advice and assistance in solving complex cases.

1.1.4. Exchange of information: reporting and follow-up

It is important that reporting authorities provide full and prompt information about follow-up of cases of suspected fraud.

Most Member States[6] have not experienced weaknesses in their reporting practices. Those that have identified issues report that most difficulties arise from lack of information and/or resources. They mentioned the following measures as helping to correct issues with follow-up:

- provision of better guidelines / adequate information to managing authorities;
- continued monitoring of implementation and reporting:
    - analysis of implementation;
    - measures to ensure correct reporting;
- collaboration between involved authorities and stakeholders

Some Member States[7] also encountered difficulties in following up on investigated fraud cases. Most[8] stated that the information flow between judicial and reporting authorities has (partly) improved.

Cooperation and communication agreements, roundtables or working groups, and continued monitoring arrangements have been set up to improve the exchange of information.

[6] AT, BE, CY, DE, DK, FI, FR, HR, HU, IE, LT, LU, MT, NL, PL, PT, RO, SE, SK.

[7] BG, CY, CZ, DK, EL, HR, HU, IT, LV, PL, SE, SI, SK.

[8] CZ, BG, DK, EL, HU, IT, LV, PL, SE, SK

.

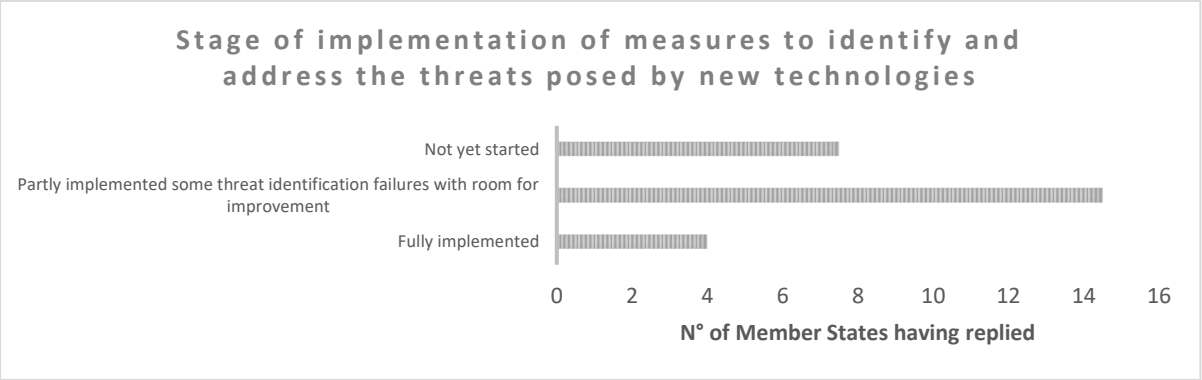
1.2. Recommendation 2: digitalisation of the fight against fraud high on Member States' agenda

Member States should ensure that digitalisation of the fight against fraud is part of their NAFS. That approach should define strategies to:

- ***i.*** *identify existing and future threats arising from new technologies:*
- ***ii.*** *develop the necessary IT architecture (inventorying existing tools, developing new ones, ensuring appropriate interoperability between them); and*
- iii. *identify and address existing gaps, also in terms of the skills needed.*

Technological developments facilitate many aspects of our lives, including the fight against fraud. However, it also poses potential threats. Therefore, it is important that Member States address the challenges posed by these technological developments. National anti-fraud strategies (NAFS) should include measures to identify existing and future threats arising from new technologies. While most Member States[9] have acknowledged this issue, several[10] have not yet integrated digitalisation as part of their NAFS.

While a few Member States[11] have already fully implemented measures to identify and address the threats posed by new technologies, most[12] have implemented only some measures, so they need to continue investing in innovative measures.



1.2.1. Implementation

Most Member States have adopted a strategy to develop their IT architecture by taking inventory of existing tools, developing new tools and ensuring interoperability between them (see next table). Many Member States are continuing to invest in updating and developing existing IT tools, in particular Arachne.

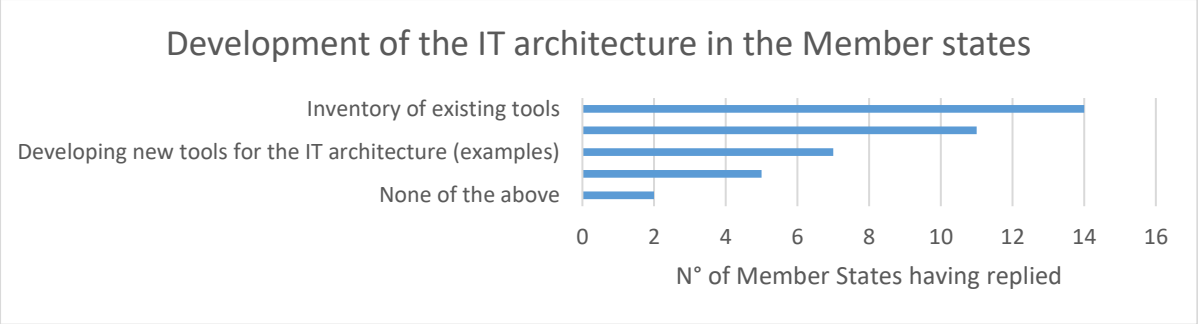
As several Member States have just started to implement their NAFS, it is important that the use of IT tools is integrated in it from an early stage on.

[9] AT, BE, BG, DK, EE, EL, ES, FR, HU, IT, LU, LV, LT, MT, PT, SI, SK.

[10] CY, CZ, DE, FI, HR, NL, PL, RO, SE.

[11] DE, IT, PL, RO.

[12] AT, BE, BG, CZ, DK, EE, ES, FI, FR, HU, LV, LT, PT, SE, SI.



1.2.2. Addressing gaps in digitalisation

Over half of the Member States[13] indicated that they have taken steps to identify and address skills gaps in digitalisation, most of which referring to gaps due to a lack of information and/or access to data on digitalisation. Measures to address these gaps often revolve around knowledge sharing, training, broadening know-how and skills, and continued development of existing systems.

[13] AT, BG, CZ, DE, DK, ES, FI, IE, IT, MT, PL, PT, SE, SI, SK.

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

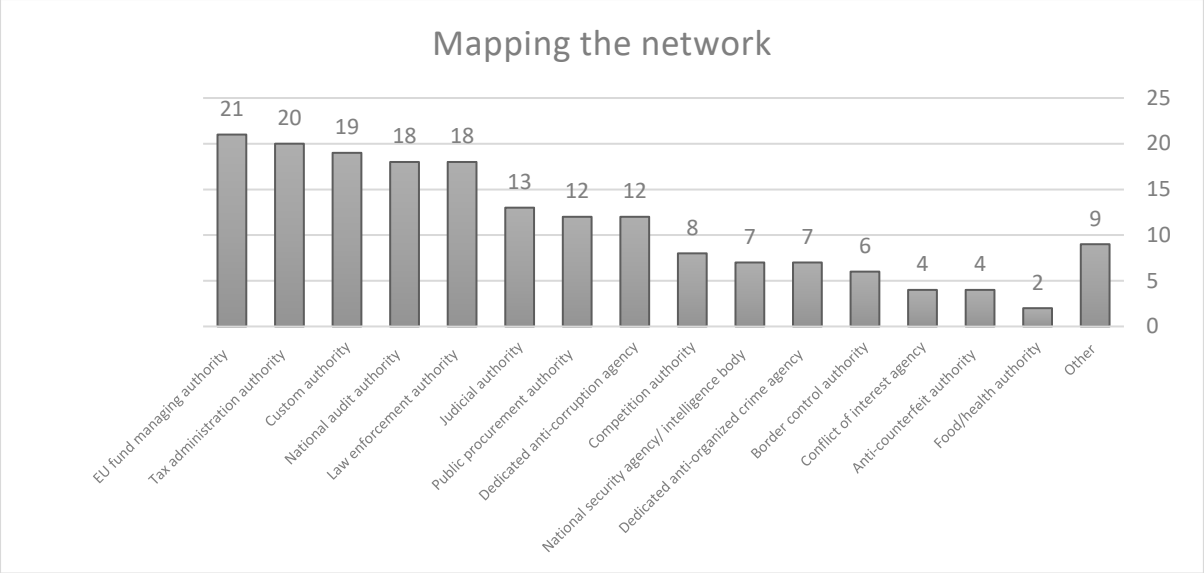
National anti-fraud networks have been developing in several Member States, with the national anti-fraud coordination services (AFCOSs) playing a key role. The Commission supports and encourages this process, which should be extended to all actors concerned, involving the relevant law enforcement and judicial authorities at national and European level. Member States should also ensure that the national structures coordinating this process are properly staffed.
Anti-fraud networks provide the ideal structure for the development and updating of NAFS.
The commission reiterates its recommendation that the Members States which have not yet adopted a NAFS should do so.

Most Member States[14] either have an anti-fraud cooperation network linking many different bodies or are developing one. According to the survey, the following agencies are most commonly represented in the national anti-fraud networks: EU fund managing authorities, tax administration authorities, custom authorities, national audit authorities and law enforcement authorities.

The table below shows the various types of agency that are part of national anti-fraud networks and how many national networks contain an agency of that type. Additionally, almost all Member States actively cooperate with EU-level judicial and investigative bodies, in particular with OLAF and the EPPO.

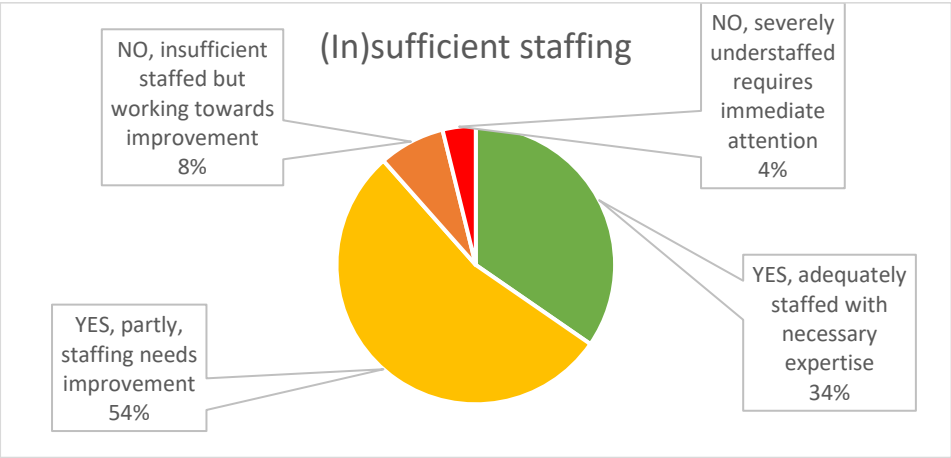
Regarding the degree of involvement, most Member States[15] say their national law enforcement and judicial authorities are actively involved in and cooperate in their national anti-fraud network. Several other Member States[16] report only moderate cooperation here, with room for improvement.

[14] AT, BG, CY, CZ, DE, DK, EE, EL, ES, DI, FR, HR, HU, IT, LV, MT, PL, PT, RO, SE, SI, SK
In development: BE, NL, IE, LT.
[15] BG, CY, CZ, DE, ES, FI, FR, HR, HU, IT, MT, PL, RO, SE, SI, SK.
[16] BE, DK, EE, EL, LV, NL, PT.



1.3.1. Staffing

Most Member States[17] have sufficient staff in their national anti-fraud coordinating structure. Most also note a need to improve their staff's expertise level, through training, new guidance on procedures, and by bringing staff from the various executive and investigative bodies together.



[17] Adequately staffed with necessary expertise: AT, BG, CZ, DE, DK, EL, HU, IT, SI
Staffing needs improvement: CY, EE, ES, FI, FR, LU, LV, MT, NL, PL, PT, RO, SE, SK.

2. Replies from the Member States

Improving the detection, reporting and follow-up of suspected fraud

Q.1.1 Do you assess your Member State as having a low incidence of fraud?

Most (63%) of the Member States who participated in the survey assessed their country as having a low incidence of fraud for the reasons outlined in the table below (Q1.2).

	Member State	**TOTAL**
Yes	AT, BE[18], BG, CZ, DE, DK, EL, ES, FI, HR, HU, IE, LV, LT, MT, NL, PT, SK	17
No	BE[19], CY, EE, FR, IT, LU, PL, RO, SE, SK	10

Q.1.2 Can you explain why? Which measures have been adopted to determine the incidence of fraud?

MS	**Input**
AT	- Strengthening **international networking and cooperation** - Developing **digital processes** - **Simplifying legislation** (taxation + customs)
BE	ERDF Wallonia: - Prevention and detection measures in place - Extensive administrative and on-the-spot-**checks** on every operation - Efficiency of systems, as confirmed by the error rates calculated by national and Commission auditors in relation to the ERDF programme ERDF Brussels Capital Region (BCR): - **Checks on payment claims** before they are sent to the European Commission - Beneficiaries are **well informed in advance of the applicable regulation and the verifications** done by authorities. Federal Public Service (FPS) FINANCE Customs and Excise *(Administration Générale Douanes et Accises - AGD&A*): - Measures taken based on the irregularities and fraud cases reported in **OwnRes.**
BG	- Cases of irregularities are classed as suspected fraud at the stage where the Bulgarian Prosecutor's Office or the European Public Prosecutor's Office initiates **pre-trial proceedings** for a criminal offence of a general nature. - When the behaviour at issue is also classed as fraud as part of the pre-trial proceedings, evidence is collected to establish whether fraud has been committed. - In a few cases, the Prosecutor's Office and EPPO do not provide the managing authorities with information promptly when pre-trial

[18] ERDF Wallonia, ERDF RBC.
[19] FPS FINANCE AGD&A.

	proceedings have been initiated. This should not automatically be considered a weakness as the Prosecutor's Office has a variety of reasons and grounds for not providing information during pre-trial proceedings.
CY	- All audit and control bodies are **instructed to report** cases of suspected fraud to the Cypriot AFCOS where those cases involve EU funds (expenditure side). All such cases are reported to OLAF through the **IMS**. - The audit and control authorities report cases of suspected fraud for further investigation either to OLAF, the EPPO, the national anti-corruption authority or the public prosecutor's office (to be investigated by the police and subsequent penal proceedings).
CZ	- Anti-fraud measures include the level of **law enforcement; cooperation among law enforcement authorities; the legal environment; the implementation of experience and good practices of other European countries.** - The low incidence of fraud in the implementation of the ESIF can be attributed to a robust methodological and control system that includes elements to combat corruption and fraud. - The **administrative verification** of payment applications and project implementation reports, supplemented by **on-the-spot checks** (both at the time of project implementation and during the sustainability period) have proved to be effective measures. A risk analysis for on-site controls, which includes screening in Arachne, indicates projects with potentially higher risks. - Other good practices include a **four-eyes check** and having external bodies (audit authority, supreme audit office) involved in the audit. - If prosecuted, suspected criminal offences such as fraud are **reported as irregularities via IMS** MS2014+ (IRQ3). This ensures that other relevant bodies (such as the paying authority and audit authority) are informed. - In case of fraud, cooperation with the Czech police is built up gradually (through **written, electronic or telephone communication)**. - Checks are run in the **Arachne** system in particular before any decision on granting a subsidy or in other activities. The **CRIBIS** system, the register of beneficial owners, etc. are also used. - Increased emphasis on **identifying the beneficial owners of companies and avoiding conflicts of interest.** - Continued efforts to **update the measures** needed to adequately respond to increasingly sophisticated attempted fraud.

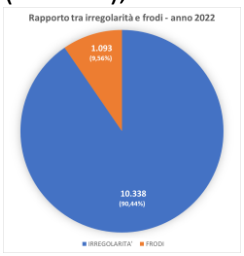
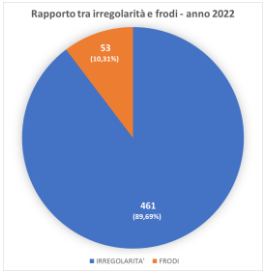
DE	- **Regular information exchanges with managing and audit authorities,** based on IMS data and the associated explanatory notes from the reporting units. Examples ERDF managing authority for Baden-Württemberg - The scope and depth of auditing by the **authorising body (*L-Bank*),** which must comply with the Federal Financial Supervisory Authority's strict requirements on banking supervision**.** Federal State of North Rhine-Westphalia - Standardised processes and procedures and organisational security features such as functional separation or the **6-eyes principle** ensure that errors and irregularities occur far less frequently. - Chapter X.2 of the 'Guidelines on fraud risk assessment and on effective and proportionate anti-fraud measures' explains how to notify irregularities and fraud cases. The German prosecutor's office and, where appropriate, the EPPO are also notified in fraud cases). Federal State of Rhineland-Palatinate - The *Land* analyses and evaluates the annual reports of the Rhineland-Palatinate Court of Auditors, the European Court of Auditors and the ERDF audit authority. Any new risks identified are integrated into the **Rhineland-Palatinate fraud prevention tool.** Federal State of Schleswig-Holstein - Schleswig-Holstein follows the recommendations for 2021-2027 set out in the European Commission guideline '**Fraud risk assessment and effective and proportionate anti-fraud measures**' and takes a proactive, structured and targeted approach to dealing with fraud risks.
DK	- The Danish Business Authority has numerous registers for running digital checks and comparisons. These produce **awareness lists used for manual checks** e.g. on payment of wages and double funding. - The Danish Fisheries Agency states that every case involving a request for payment has two case handlers **who check each other's work**. The Agency reported thorough controls, approved by the Auditing Body several times, most recently in 2023. In addition, there is legal support when necessary. - The Danish Agricultural Agency reported a 'No' in Q.1.1, [i.e. high incidence of fraud] as Danish fraud detection rate (FDR) for the common agricultural police (CAP) is significantly above the EU average.
EE	- The revenue department assesses the incidence of fraud as low, due to the risk-detection activities and identification of possible customs duties. - However, the actual incidence is probably significantly higher due to the hidden nature of fraud,**which makes it hard to identify, detect and prove**. - Estonia is currently improving risk assessment, analysis, and cooperation between concerned authorities by organising **training courses and workshops, compiling guidelines, etc.**
EL	**Financial Audit Committee:** All bodies of the Greek management and control

	system, including EDEL, contribute to the implementation of the national anti-fraud strategy and as part of their audit activities include a set of fraud prevention and response actions. Procedures have been included in the Greek management and control system (MCS) concerning: **(a)** an assessment of fraud risks, in the context of the prevention and implementation of effective and proportionate anti-fraud measures in structural actions; **(b)** examination of signs of fraud and reporting suspicions of fraud by the managing authorities (MA) / intermediate bodies (IB) / certifying authority (CA), in the context of the application of the MCS procedures and the exercise of their responsibilities; **(c)** receiving and examining complaints concerning co-financed programmes/projects; and **(D)** assessing and addressing risks that may affect the smooth implementation and achievement of objectives of the operational programmes. The implementation of the above MCS procedures ensures, on the one hand, the prevention of fraud/suspicion of fraud and their timely detection by the competent national audit bodies. In particular, EDEL, as the audit authority for co-financed programmes and as the supreme national audit body, checks, through system audits, the existence of the necessary procedures and measures to prevent and deal with fraud by the managing bodies (assessment of Key Requirement 7 '*Effective implementation of proportionate anti-fraud measures'*), and through audits of operations, the existence of a possible suspicion of fraud in the implementation of the audited operations. If suspected fraud is detected by system and operations audits, EDEL informs OLAF, as well as the competent national authorities (AFCOS, etc.) via IMS, about the launch of the necessary procedures to detect fraud or not. Similarly, the MAs, IBs, CA, from their audits/verifications and applying the above-mentioned MCS procedures, inform OLAF and the competent national authorities, in case of detection of suspicions of fraud. All the relevant MCS bodies cooperate closely and systematically with the NTA, which has the role of coordinator (AFCOS) in the fight against fraud in Greece. In view of the above and considering that MCS bodies, including EDEL, can only detect suspected fraud, while fraud is established by other control bodies as well as the judicial authorities, the low incidence of suspected fraud is due to the low levels of cases of fraud detected by MCS bodies during their audits. **Special Service for Institutional Support and Information Systems:** For actions financed by the NSRF, the MCS provides, in the procedures and forms, for measures which have also reduced risks of fraud in PP 2014-2020 and PP 2021-2027. For example, the establishment of the obligation to declare no conflict of interest and beyond for all staff of the Managing Authorities and Intermediate Bodies, measures in the NSRF Integrated Information System for non-double funding, the operation of an Internal Anti-Fraud Network with the participation of all Managing Authorities and cooperation with AFCOS in the handling of complaints relating to co-financed operations. **Recovery and Resilience Facility Coordination Agency**: All projects financed by the Recovery and Resilience Fund are subject to ex-ante or ex-post control

	procedures, which form a coherent management framework which, on the one hand, acts as a deterrent to the recipient of funding, and on the other hand allows irregularities to be detected in a timely manner, including those that may involve fraud.
ES	- The number of cases of suspected fraud reported in the IMS is very low. This could be because **proper management and control systems are in place, although there is room** for improvement. - As a result of the implementation of the **recovery, rransformation and resilience plan**, all Spanish public administrations that manage these funds – at state, regional and local level – have adopted anti-fraud plans containing numerous measures for protecting financial interests at different stages of **the anti-fraud cycle.** These include: having institutional anti-fraud statements for each entity; approving codes of ethics and public integrity; setting up anti-fraud committees and internal control units; assessing the risks of fraud, corruption, conflicts of interest and double funding; planning and performing anti-fraud controls based on red flags, implementing procedures to prevent and address conflicts of interest; and creating **internal whistleblowing** channels.
FI	- Only a few suspected cases of fraud are found during controls and audits of EU-funded programmes. **Controls are carried out regularly** on the basis of anti-fraud strategies or anti-fraud plans and risk assessments drawn up by the authorities in charge of the different programmes. The EU programmes managed by Finland are audited regularly, not only by national authorities but also by EU institutions such as the Commission and the European Court of Auditors. In light of the audit results, there is no reason to suspect that there are in reality many more cases of fraud involving EU funds or that the authorities fail to detect a substantial number of such cases. - Finnish Customs consider the risk of fraud to be generally low in Finland, which has a low level of corruption, as evidenced also by international comparisons. However, Finnish Customs do detect cases of fraud that are similar to those identified by law enforcement authorities in other Member States. This can be explained by the **EU's common customs code and customs duties.** Finland is smaller than many of the other EU Member States, making it difficult to compare countries. - In addition, Finnish Customs' analysis and intelligence unit, in particular the unit for checking marketing risks, focuses on fraud prevention and risk analysis, among other issues. Anti-fraud analyses always include **a fiscal risk analysis**. For example, all anti-dumping tax issues and analyses in this area are well modelled and allow possible cases of fraud to be detected under Customs' supervision.
FR	Suspicions of fraud exist and are found during the concomitant checks carried out by the paying agencies, as well as during *ex post* controls carried out by Customs and the 'COSA' team responsible for controls on operations in the

	agricultural sector. Depending on its degree and severity, fraud may be classified as administrative and subject to a fine or classified as criminal and reported to the public prosecutor in accordance with Article 40 of the Code of Criminal Proceedings. It is up to the public prosecutor to investigate compliance with the law or launch criminal proceedings for fraud.
HR	Contribution from the Ministry of Agriculture: – Functioning of the **management and control system** – Risk analysis for irregularities and/or fraud – **Staff training on** spotting red flags, reporting suspected irregularities and **taking timely action** Contribution from the Ministry of Agriculture - Directorate of Fisheries - We believe that fraud in connection with the European Maritime and Fisheries Fund (2014-2020) and the European Maritime, Fisheries and Aquaculture Fund (2021-2027) is infrequent, given that (a) just one case of irregularity with elements of suspected fraud has been recorded in Croatia since the start of implementation of both funds, and (b) DG MARE's audit of key requirement No 7 of the management and control system for the 2014-2020 period, i.e. 'Effective implementation of proportionate anti-fraud measures'. found no deficiencies in the management and control system, which was classified under Category 1 (Works well. No or only minor improvement(s) needed.). Contribution from the Customs Administration (Ministry of Finance) - For risk analysis, the low incidence of fraud could be attributed to the **risk analysis system being overwhelmed by the incorrect activation or non-activation of risk rules** (based on both national and EU rules). This often results from incorrectly completed customs declarations (e.g. incorrect recording of non-structured data such as the trade name, goods description or address), since entering some data is optional. This is prevented through **detection of permutations of a targeted risk indicator**, which inevitably results in the system becoming overwhelmed. - The measures taken include **cooperation with the customs authorities of other Member States,** continuous monitoring of the quality of data in customs declarations submitted, implementation of risk analysis for every change made to a declaration, as well as cooperation in customs matters **with the EU Member States, non-EU countries, the World Customs Organization, Europol, and OLAF** for the exchange of useful operational information. - The measures taken as part of *ex post* checks planning include **improving the efficiency of searches in our own databases and the databases of other bodies**. Public source data and information on persons and events that could be of interest are also collected. An additional risk analysis is carried out to select bodies for *ex post* checks. This look at any irregularities detected (in relation to value, tariff, origin, anti-dumping violations, etc.) Contribution from the Tax Administration (Ministry of Finance): - Performing risk management operations relating to non-compliance with

	tax obligations, using the compliance and risk management system (CRMS) owned by the tax administration - Conducting **risk analysis** - Developing and improving **digital transformation**
HU	- The number of criminal proceedings initiated by the institutions managing EU funds has been low. - **Thematic training** has been provided and anti-fraud information materials have been produced for staff working in the field of development policy.
IE	Cases of fraud and irregularities in cohesion funding for Ireland decreased in 2014-2020 period. Government policy is implemented and public services are delivered at multiple levels across the Irish public service. Therefore, there is a well-established **framework for accountability, responsibility and control in operation**. This framework encompasses the role of the Comptroller and Auditor General, the public financial procedures (PFPs) and requirements for governance, and the institutional and financial relationships between parliament and the executive. The PFP published by the Department of Public Expenditure, NDP Delivery and Reform, sets out the main principles of government accounting and the primary ways they are applied in the day-to-day operations of government departments and offices. They are a practical guide to assist officials in understanding the financial framework and the need to promote good practice and high standards of propriety in all financial matters. The 1997 Public Service Management Act provides the central accountability framework setting out the formal structure for assigning authority and accountability within the civil service. The Accounting Officer is personally accountable to the Parliamentary Committee of Public Accounts (PAC) for regularity and propriety in relation to public resources and value for money. This is provided by means of rigorous *post factum* examination and independent audit and examinations by the Comptroller and Auditor General and scrutiny by the PAC. As the systems in place may not have general application, some specific examples are included below. All the projects included in Ireland's national recovery and resilience plan (RRP) are covered by the above which provides assurance in relation to the measures to protect the EU's financial interests. There are specific requirements in place for the RRF. The governance structures here include a delivery committee and the Project Leads Network to ensure compliance. There is also a memorandum of understanding with the accountable departments which includes obligations in relation to the protection of the EU's financial interests. The accountable department must ensure adequate controls are in place for preventing, detecting and correcting fraud, corruption and conflicts of interest. RRF projects in Ireland are pre-funded by the Exchequer. If an irregularity is identified in an RRF-funded project, the financial correction will generally not be recovered directly from the final beneficiary (unless for example, it is due to fraud or corruption), but will be addressed either by an adjustment to the RRF payment instalment or through a refund to the EU. Training on this has been provided to the accountable departments. Work is

	ongoing to enhance the audit and control systems in fraud risk assessment and reporting skills With respect to the ERDF co-funded regional programmes for 2014-2020, expenditure was checked extensively at intermediate body and/or managing authority level before being submitted to the certifying authority. While management verifications did result in financial corrections, none of these related to suspected fraud. The expenditure included in payment claims and the management and control systems for the two 2014-2020 ERDF regional programmes have also been extensively audited by national and Commission auditors. While the audit work did identify irregularities, there have been no findings in respect of fraud or suspected fraud. The ERDF managing authority staff completed training on fraud risk and made early, if limited, use of ARACHNE, the Commission's data-mining tool. Irregularities were reported using the AFIS-IMS. Likewise, for the ESF, there are well-established and mature reporting structures. The type of expenditure declared for this (payroll related) retrospective declaration mitigates risk of fraud.
IT	The assessment in reply to question Q.1.1. is based on general data from the 2022 PIF report on overall irregularities/fraud relating to own resources, cohesion policy and fisheries and common agricultural policy. Specifically, at EU level, out of 11 431 reported cases, 10 338 were irregularities (90.44%), and 1 093 related to fraud (9.56%).  In Italy, out of 514 cases, 461 were irregularities (89.69%), and 53 related to fraud (10.31%).  Thus, in terms of fraud detection, Italy's figure is fully in line with the EU average and only slightly higher. Determining the incidence of fraud, strictly in terms of numbers, is part of the daily work carried out at the various levels by the national and local authorities engaged in protecting the EU's financial interests (managing authorities, audit bodies, intermediate bodies, paying agencies, law enforcement agencies, control authorities, etc.), through comprehensive analysis and control models. These models are based on the directives issued from time to time as part of the national anti-fraud strategy, by the Committee for the Prevention of Fraud against the EU (which are periodically updated in light of new developments) and the daily monitoring activities carried out by the network of national liaison

officers to control, support and improve the quality, consistency and correctness of the data in IMS.

To cover the eventuality that the question may be broader and cover measures to detect and discover fraud, below we provide clear and comprehensive information on the overall **structure of the fraud prevention and response system** currently in place in Italy, with reference to major regulatory and organisational measures taken by the EU institutions, so as to highlight its effective potential in terms of both **deterrence** and **response**.

In particular, the **key strengths of the Italian system** are set out below.

Full and effective implementation of Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law, also known as the PIF Directive. This was first transposed into the national legal system by **Legislative Decree No 75 of 14 July 2020**, which broadened the scope of several offences to strengthen the criminal law response to fraud and other offences against the EU. This was complemented in 2022, first by **Decree-Law No 13 of 25 February 2022** (later repealed by **Law No 25 of 28 March 2022**, which, however, reproduced the part relating to the PIF Directive regulations), and then by **Legislative Decree No 156 of 4 October 2022**.

The **main contents** of the legislative amendments can be summarised as follows:

- the categories of payments that may be exposed to criminal conduct affecting the EU budget have been expanded;
- the offence of international bribery/conspiracy under Article 322-bis of the Criminal Code has been strengthened;
- criminal liability has been introduced for the attempt to commit certain tax offences, if cross-border in scope and causing a total loss of EUR 10 million or more;
- the administrative liability of entities for tax offences has been aligned with the description of the EU cross-border dimension relevant for PIF purposes;
- the scope of asset seizure measures against fraudsters has been expanded, by introducing the confiscation of 'disproportionate assets' in cases of aggravated fraud affecting the EU's financial interests and aggravated fraud to obtain public funding, confiscation of equivalent assets in smuggling offences, and confiscation of equivalent assets and confiscation of disproportionate assets for the offence of misappropriation of agricultural aid payments.

Consequently, a **strong and comprehensive framework of penalties** has been put in place, able to effectively target all types of offences against the EU's financial interests, on both the revenue and expenditure sides, as well as related corruption and money laundering and involvement of criminal organisations.

Comprehensive legislative measures have established effective tools for **seizing the assets of fraudsters**, such as **direct confiscation, confiscation of equivalent assets and disproportionate assets**, and are applicable (in the form of seizure) even during investigations. Furthermore, the **interim asset seizure measures under the anti-mafia legislation** have been made applicable (even before a final guilty verdict is delivered) not only against suspected organised crime members but also against individuals having unjustified wealth who are found to habitually

	engage in economic and financial crime (hence including crimes against the EU's financial interests); The legislation on the **European Public Prosecutor's Office** has been **fully implemented**. This legislation was transposed in Italy by **Legislative Decree No 9 of 21 February 2021** and by a series of agreements and initiatives between the Italian Ministry of Justice and other national institutions that have enabled the European Delegated Prosecutors in Italy to fully perform their functions. The data in the **2022 EPPO Annual Report** show that, among EU countries, **Italy proves the strongest cooperation with the EPPO**, in terms of resources and investigative capacity. The report shows that **at the end of 2022 Italy had 16 active European delegated prosecutors, the highest number in the EU**. Italy also had the **highest number (45)** of **national European delegated prosecutors' assistants**. This (in conjunction with point (e) below) explains why, as stated in the 2022 EPPO Report, **Italy** had the **highest number of active investigations** by European Delegated Prosecutors (285, of which 275 were opened in 2022). A **comprehensive institutional mechanism has been established to ensure full and widespread monitoring of all the areas requiring protection of the EU budget** (own resources, common agricultural policy, cohesion policy), made up of agencies, ministerial departments, managing and audit authorities, paying agencies, police forces and the judiciary. The **Committee for combating fraud against the European Union (COLAF)**, operating as the Italian anti-fraud coordination service, offers those bodies a permanent forum for discussing issues and exchanging information. The COLAF was established by Law No 142 of 19 February 1992 (later updated and supplemented with further functions). This means that Italy has a track record of over 30 years of interinstitutional cooperation to protect the EU's financial interests. The legislation gives the **Financial Police (*Guardia di Finanza*)** specific competences, control powers and specialised human resources for **economic and financial policing**, including for the **protection of the EU's financial resources**. To cover this area, the Financial Police has specialised units, including the central **Public Expenditure and Anti-EU Fraud Unit (*Nucleo Speciale Spesa Pubblica e Repressione Frodi Comunitarie*)** and a local network of **public expenditure protection groups** belonging to **Economic and Financial Police Units**. During the presentation of the EPPO 2022 Report to the joint meeting of the CONT and LIBE Committees in March 2023, the **European Chief Prosecutor**, **Laura Codruța Kövesi**, voiced her appreciation for the Italian model stating, 'if we can replicate Guardia di Finanza in all the Member States I would be happy to do this thing, because they have a lot of professional investigators dedicated to the EPPO cases and this is why we have these good results'; **Very broad judicial police powers** and **administrative powers, including access and inspection authority** have been put in place. In this context, national legislation provides, among other things, that the **Financial Police** may use all the investigative powers given to them – including access, inspection, search and the

	sending of questionnaires – to prevent and prosecute infringements in tax matters and to prevent and combat infringements in the fields of custom duties, border charges and other own resources and expenditure from the EU budget. A specific branch of the Financial Police, the **Public Expenditure and Anti-EU Fraud Unit**, was granted additional powers by Law No 161 of 30 October 2014, which added paragraph 1-bis to Article 25 of Decree-Law No 83/2012. This provision states that in order to carry out 'analyses, inspections and controls on the use of resources from the budget of the State, regions, local authorities and the European Union', the Unit may consult the Financial Relationship Archive and exercise the powers conferred on it by currency law (including the power to request from banks and financial intermediaries documentation on the parties concerned, access public, business and commercial premises to carry out inspections, checks and searches, and delegate the above checks on expenditure flows to the local units of the Financial Police, by granting them the latter powers). An effective regulatory framework governs the administrative liability of entities for criminal offences, and is also fully applicable to criminal conduct affecting the EU's financial interests. Comprehensive prevention systems are in place against corruption (including the functions of the National Anti-Corruption Authority, the three-year anti-corruption plans and whistleblowing legislation) and money laundering (especially through the reporting of suspicious transactions). The **fraud risk analysis and assessment** systems and procedures set up by the EU institutions have been fully implemented and are served by independent and innovative information systems. In the field of fraud risk analysis and assessment, the national framework fully meets the need to prevent and combat fraud against the EU. Over time, every institution and agency responsible for managing EU resources for any reason has set up a number of systems, applications and databases, together with methods and procedures, for the appropriate prior assessment of the risks of fraud, corruption, conflict of interests and double funding linked with implementation of the EU budget. With regard to **cohesion policy**, risk assessment is one of the main control functions of the various managing authorities. For this purpose, they follow closely **the Commission's EGESIF Guidance Note No 14-0021-00 of 16 June 2014** on '**Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures**'. They also rely extensively on the **ARACHNE** system, in accordance with the '**National Guidelines**' produced by a dedicated national working group set up within the State General Accounting Department of the Ministry of the Economy and Finance. Also at national level, the **Inspectorate General for Financial Relations with the European Union** in the State General Accounting Department, which coordinates audit authorities and their functions, has issued a '**Manual of Audit Procedures**' (Version 7 of 21 July 2021), which includes a section on risk assessment. To increase the effectiveness of measures to prevent and combat fraud against the EU budget, in 2022 the **Financial Police** directed the evolutionary maintenance of **SIAF (Anti-Fraud Information System)**, an application

implemented under a project financed with resources from the 'Governance and Technical Assistance 2007-2013' national operational programme. SIAF is a business intelligence platform that supports operational analyses in the field of public expenditure. Uploading the data acquired from the other databases used by the Financial Police to this system makes it possible to extract lists of public funding beneficiaries potentially at risk of irregularities. This resource, initially only available to the Financial Police Units located in the convergence objective regions of the 2007/2013 Multiannual Financial Framework (Puglia, Campania, Calabria and Sicily), was extended to the whole country in 2021.

An important addition to the toolbox of measures Italy put in place to step up risk analysis in EU fund management is the **Integrated Anti-Fraud Platform (PIAF-IT)**. Created by the State General Accounting Department in collaboration with the COLAF, using resources from the EU's Hercule III Programme, the platform extracts useful information from the massive data banks held by national and local authorities. Specifically, PIAF-IT is an integration platform that extracts, aggregates and reconciles data from national sources (Revenue Agency, the Chamber of Commerce Information System - Infocamere, Italian Court of Auditors) and European sources (IMS and the Financial Transparency System - FTS) to generate fact sheets on natural or legal persons, supporting the assessment of possible frauds, so as to:

- intensify the exchange of information and thus maximise the fraud prevention phase;
- centralise and make visible all key information on beneficiaries of EU public funding;
- develop specific analysis outputs of said information via comparison with data in other databases by querying a single information system, in an aggregated manner, without having to make several separate queries.

The platform can also be an effective support tool for ARACHNE to consolidate and strengthen the fight against irregularities and fraud and other illegal activities against the EU budget both before expenditure certification and in the *ex post* control phase, as well as during administrative controls on implementation of the national RRP.

The technical context of PIAF-IT, which includes a microservices architecture enabling it to store big data, has the following additional functionalities:

- it can be used to make online searches (ordinary and historical views of a natural or legal person) and generate and display detailed information sheets;
- it can be extended to other data sources in future for an even better analysis of the subjective and objective elements of the position to be examined. (Examples of these sources include the Ministry of Justice's Criminal Records Information System on past convictions for fraud against the national and EU budget, and the Kohesio database managed by the Commission's DG for Regional and Urban Policy (DG REGIO), which has up-to-date information on projects and beneficiaries co-financed by the EU cohesion policy.)

The **risk analysis** framework described above is at least partly responsible for the low incidence of fraud in the cohesion policy sector in Italy, even though in

general terms, as we have seen, the overall incidence of fraud against the EU budget in Italy cannot be said to be low.
Since 2015, significant progress has been made following the Commission's issuing of EGESIF guidance and its application in Italy, together with the extensive use of Arachne, supported by best use procedures developed by a dedicated national working group. These objective factors may have contributed to the decrease in fraud in this sector compared to previous periods.
Moreover, the low incidence of cohesion policy fraud out of the total number of irregularities detected in European Structural and Investment Funds (ESIF) is a feature that Italy has in common with a number of other Member States, as shown by the breakdown tables in the 34th PIF Report 2022. The report shows that, in the year in question, with regard to fraud against cohesion policies, Italy and **8 other Member States** (Belgium, Ireland, Spain, Lithuania, Luxembourg, Malta, Austria and Finland) had **no fraud cases**, while **5 countries** (Slovenia, Cyprus, Portugal, Greece and the Netherlands) reported **only 1 case of fraud**.
This incidence was largely similar across the past 5 years, as shown by the annexes to the PIF reports for the period 2018-2022; specifically:

- in 2018, **Italy** reported (in the areas of cohesion policies and fisheries) **only 1 case** of fraud, as did **6 other Member States** (Austria, Belgium, Bulgaria, Cyprus, Spain, Sweden), while **5 countries** (Ireland, Luxembourg, Malta, Netherlands, Slovenia) **reported no cases of fraud**;
- in 2019, **Italy** reported **no cases of fraud** (in cohesion policies and fisheries)**,** as did **10 other Member States** (Belgium, Cyprus, Croatia, Denmark, France, Greece, Ireland, Luxembourg, Malta, Sweden), while **1 country (Bulgaria)** reported **only 1 case** of fraud;
- in 2020, **Italy** (in cohesion policies and fisheries) reported **3 cases of fraud** as did **6 other Member States** (Croatia, Estonia, Greece, France, Slovenia, Sweden), while **1 country** (Bulgaria) reported **2 cases**, **2 countries** (Cyprus and the Netherlands) reported **1 case** and **7 countries** (Austria, Denmark, Finland, Lithuania, Ireland, Luxembourg, Malta) reported none;
- in 2021, in relation to cohesion policies, **Italy reported no cases**, as did **11 other Member States** (Austria, Cyprus, Croatia, Denmark, Finland, Ireland, Luxembourg, Malta, Slovenia, Spain, Sweden), while **1 Member State** (Belgium) reported **only 1 case** of fraud.

In addition to the framework described above, measures were introduced specifically to **detect fraud against the national RRP** and related corruption, conflicts of interests and double funding.
Under **Article 6** of **Decree-Law No 77** of **2021**, converted by **Law No 108 of 2021**, as amended by **Decree-Law No 13** of 2023, converted by **Law No 41 of 2023**, the protection of the EU's financial interests in implementing the national RRP under Article 22 of Regulation (EU) No 2021/241 is entrusted **to the Inspectorate General for the national RRP** at the **State General Accounting Department.**
The Ministry of the Economy and Finance issued **guidelines on the control and reporting of national RRP measures (circular No 30** of **11 August 2022)** and later supplemented the guidelines **(circular No 16 of 14 April 2023).** The guidelines are addressed to the central administrations and implementing entities, and cover

	the administrative management and implementation of the RRP. With regard more specifically to preventing and combating outright fraud, the **Decision of the State General Accounting Department of 9 March 2022** set up a **network of national RRP anti-fraud contact points**, to coordinate the **periodic assessment of fraud risks, conflicts of interests and double funding**, and to plan **effective and proportionate measures**. The network is chaired by a senior official of the national RRP General Inspectorate and is composed of representatives of the Inspectorate and of the **Financial Police**, plus an anti-fraud contact person designated by each central administration in charge of NRRP measures. The network works in close contact with the competent national institutions with regard to anti-corruption, anti-money laundering and public expenditure control, such as the **National Anti-Corruption Authority**, the **Bank of Italy's Financial Intelligence Unit** and the Italian **Court of Auditors**. Depending on the issues on the agenda, the Network's meetings are also attended by experts and representatives of the COLAF, other State and EU bodies, other national public administrations and bodies, offices of the State General Accounting Department or other departments in the Ministry of the Economy and Finance, as well as public and private companies, trade associations, and other bodies and organisations concerned. The network also implements cooperation under the **Memorandum of Understanding signed on 17 December 2021 between the State General Accounting Department and the General Command of the Financial Police**. This cooperation is outlined below. - **The national RRP General Inspectorate** forwards the **Public Expenditure and Anti-EU Fraud Unit of the Financial Police** detailed information and findings regarding irregularities, frauds and abuses it has detected while performing its monitoring and control functions. It flags the actions and their implementing or executing entities deemed to be particularly at risk, for independent analysis and control by the Unit, providing any useful information and details; - The Public Expenditure and Anti-EU Fraud Unit relays the information to the other special units and to the operational units of the Financial Police with territorial jurisdiction for any activities under their remit. In compliance with the rules on secrecy, the Anti-EU Fraud Unit then reports the findings of the checks to the national RRP General Inspectorate for any further action. - Central administrations wishing to conclude an agreement with the State General Accounting Department and the Financial Police may do so by signing a unilateral act joining the aforementioned MoU, after appointing an anti-fraud contact person, and undertaking to: (i) participate in the work of the Network; (ii) provide the General Inspectorate and the Anti-Fraud Unit with all the information in their possession on the implementers and executors of the measures financed by the Plan; and (iii) provide the Inspectorate and the Unit with detailed information considered relevant for the prevention and combating of irregularities, frauds and abuses.

	Furthermore, the above-mentioned **Circular No 16 of 14 April 2023** announced the full release (on the **ReGiS** platform) of the functionalities enabling the public administrations in charge of national RRP measures and the implementing entities to directly issue the certifications proving performance of the relevant checks (in particular on the project selection procedure, the tender procedure and project reports). The circular also announced that **ReGiS** had been **connected** to the **ORBIS world bank** and to the **ARACHNE and PIAF – IT anti-fraud platforms**, and provided specific indications on their usefulness for risk analysis and for identifying beneficial owners. Additionally, over the past few months, the Network of Anti-Fraud Contact Points has organised a number of **training sessions** for the staff of central and local administrations and implementing bodies, to fine-tune knowledge and to enable them to use the full range of fraud analysis and prevention systems. During the training sessions, the **Public Expenditure and Anti-EU Fraud Unit of the Financial Police**, with the support of the Financial Police Unit at the Department for European Affairs of the Presidency of the Council of Ministers, acting as Technical Secretariat of the COLAF, prepared and presented detailed checklists with **specific risk indicators** applicable to either the **payment of funding** or the **execution of public works**. The checklists were made available through the ReGiS system to all central and local administrations and bodies implementing the plan, to help them improve their **independent ability to detect** anomalous situations for further investigation. This comprehensive anti-fraud framework – accompanied by other tools and recommendations useful for assessing the main risks of national RRP-related fraud, detect vulnerabilities in the existing control systems and engage all stakeholders in stepping up prevention and response levels – is detailed in the **National RRP Anti-Fraud Strategy**, drawn up in October 2022 by the Inspectorate General for the national RRP with the support of the Network of Anti-Fraud Contact Points and updated in December 2023. Italy's RRP Strategy describes the key principles and general measures for ensuring compliance with Regulation (EU) 2021/241, consistent with Article 11 of the Funding Agreement between the European Commission and Italy, in line with the general principle of sound financial management. It aims to guide the actions and measures taken by individual administrations tasked with implementing the measures, so as to ensure harmonised and effective anti-fraud solutions and practices, in particular in detecting and responding to any anomalous or illegal phenomena and conduct during the plan's implementation, as well as in the processes/activities along the life cycle of the various projects. The new RRP Strategy adopted by **ReGiS Circular 200465** of **22 December 2023** incorporates the previous version and updates it with the main intervening regulatory changes, the lessons learned in the first year of implementing the Strategy, and fruitful ongoing discussions with the competent national and EU control bodies. All the administrations in charge of RRP measures were asked to promptly implement the contents of the new document in their 'sectoral anti-fraud strategies' covering the activities under their competence, and in the operational manuals for each measure.

	Another document linked to the RRP strategy is the **Thematic Appendix** adopted by **RGS** Circular **No 27 of 15 September 2023**, entitled **'Identification of beneficial owners under Article 22(2)(d) of Regulation (EU) 2021/241 and notification to the financial intelligence unit of suspicious transactions by the public administration under Article 10 of Legislative Decree No 231/2007'**. This aims to: improve *ex ante* controls aimed at identifying any conflicts of interest of beneficial owners; strengthen information flows, for example via notifications of suspicious transactions in line with anti-money laundering legislation; and establish the procedural steps to be implemented by the implementing bodies and the administrations concerned via all the functionalities of the ReGiS information system. In this context, a major step forward has been the adoption of the ***national RRP fraud risk assessment tool***, designed to standardise the self-assessment of fraud risk in RRP measures and related management processes falling within each authority's remit. The tool is part of the comprehensive set of anti-fraud capabilities that help ensure the correct, efficient and effective functioning of each authority's management and internal control system. It also provides the information base for drawing up possible action plans setting out the new control steps and/or additional and proportionate measures to be implemented to mitigate the identified risks. Article 1(4)(f)(3) of Decree-Law No 13 of 24 February 2023 has further strengthened the Financial Police's in overseeing the national RRP implementation, by extending the possibility of concluding specific agreements with the Financial Police – already available to the central administrations in charge of the plan –to the regions, Autonomous Provinces of Trento and Bolzano, local authorities and other public entities involved in implementing the RRP. The new legislation is intended to strengthen control activities aimed at preventing and combating fraud, corruption, conflicts of interest and the risk of double funding, by leveraging the general economic and financial police functions and professional skills of the Financial Police and the inspection powers conferred on it also for the protection of EU financial resources, as mentioned above. All the **prevention measures** aimed at identifying the possible **risks of infiltration by organised crime** available under current anti-mafia legislation and falling under the competence of the Ministry of the Interior and the local Prefectures also apply to the various investments and projects connected with the national RRP.
LT	Good cooperation between administrative agencies, active work on preventing double funding.
LU	The national anti-fraud strategy is not yet finalised. However, viewed in the overall context of the Luxembourg economy and financial sector, the amounts involved point to a low incidence of fraud. This is probably due in part to the fast

	and effective exchange of information amongst the relevant authorities, which are physically located in close proximity to each other.
LV	One possible explanation is an effective internal control system which includes a set of preventive measures to reduce or eliminate the risk of fraudulent activities. A transparent and efficient management and control system of EU funds has been created in accordance with the principles of safe financial management and with zero tolerance for fraud. Responsible institutions also carry out fraud risk assessments regularly and define measures to prevent or reduce the risks of fraud. Each institution takes fraud prevention and detection measures based on its remit. It is important to detect cases of fraud and bring fraudsters to justice. 'Red flags' help to draw attention to suspicious cases. The institutions use a methodology known as 'Criminal offences against EU financial interests: definitions, typologies, signs and examples of practice' developed by the AFCOS and a crime typology filtering IT tool to detect suspicious cases. If one or more signs are detected or there are suspicions of signs mentioned in this methodology, the relevant employee consults with the management regarding further action. The number of cases has been increasing in recent years.
MT	- The Manual of Procedures stipulates that, if anyone involved in the implementation of EU funds becomes aware of an irregularity (individual or systemic) at any point during implementation or a control procedure, they **must immediately report the irregularity to the managing authority.** - One tool used to determine the incidence of fraud is a **risk assessment** aimed at pinpointing, assessing, and minimising potential dangers that could arise from deceitful actions. The Maltese managing authorities for EU funds have carried out a fraud risk assessment which resulted in the **updating of the fraud risk register**. Apart from the topics provided in the Commission memo on fraud indicators, namely 'selection of applicants', 'implementation and verification of operations', 'certification and payments' and 'direct procurement by managing authorities', other pertinent topics were also tackled. The topics included in the Fraud Risk Register include (i) the avoidance, detection and mitigation of conflict of interest, (ii) **whistleblowing,** (iii) double funding, and (iv) rules on part-time and ancillary employment. - The anti-fraud strategy has been revamped to comprehensively and clearly delineate the stages in the **anti-fraud cycle**, namely prevention, detection, investigation and correction. - A standard operating procedure has been developed for checks and verifications to be carried out by managing authorities on conflicts of interest and ultimate beneficiary owners for EU-funded contracts. - In August 2023, the Permanent Secretary responsible for EU funding sent the Permanent Secretaries a circular on conflicts of interest and action against fraud and corruption. The aim of this circular was to

	enhance the accountability, transparency and effectiveness of the measures put in place to protect the EU's and Malta's financial interests regarding the implementation of EU- funded projects. Ministries were reminded of their obligations to strengthen and carry out checks against conflict of interest throughout the design and the implementation of projects. Ministries were also asked to draw up fraud risk registers based on those aspects of operations identified as most prone to fraud and corruption.
NL	Fraud risks and the lawful use of funds (including EU funds) are important areas of focus within the Netherlands. In recent years the Dutch internal audit department has paid special attention to mitigating fraud risks and included a separate assessment of fraud risks in the audit report accompanying the justification of the ministries' annual reports. Overall, it concluded that the ministries' fraud risk management is adequate. Furthermore, the ministries have a responsibility to manage and mitigate fraud risks and take measures to prevent, detect and correct instances of fraud. The 2022 PIF report acknowledges the low incidence of fraud in the Netherlands. It points to the very small number of fraudulent transactions reported affecting the EU budget (5 expenditure transactions and 2 revenue transactions). These transactions had a total value of just EUR 40 800 for expenditure and EUR 295 800 for revenue. Hence the incidence of fraud in the Netherlands is deemed very low and is expected to remain so.
PL	The statistical data from the European Commission provided in the annual PIF reports are a reliable indicator for an objective assessment of the incidence of fraud. However, these data relate only to cases reported to the Commission in line with the notification obligation (and not to all cases of suspected and confirmed fraud, some of which were not reported, as the amounts concerned did not exceed the EUR 10 000 threshold). When compared with data from other Member States, which may serve as a benchmark, the fraud data from Poland clearly shows that Poland reports one of the highest number of fraud cases to the Commission each year, involving one of the highest the financial values. In Poland, cases are classified as suspected fraud (IRQ3) for notification to the Commission via the IMS system at a relatively late stage of the investigation process (when an indictment is issued by a public prosecutor). This is relevant for the Commission's fraud rate calculation and data analysis. Moreover, in Poland the reporting institutions are required to monitor cases of irregularities that do not have to be reported to notify the Commission. **Where indicators of suspected fraud are identified during the investigation, these are also reported via the IMS system.** This procedure is in line with the principles set out in the sectoral regulations and in the 2017 Commission manual '**Reporting of irregularities in shared management**'. In Poland's view, it does not require

	improvements.
PT	Preventive anti-fraud policies have been adopted, including: - **technical and legal analysis** of cases indicating signs of fraud and their **notification** to the competent bodies for verification; - a specific **information system** on the suitability, reliability and debt of EU funding beneficiaries; - **cooperation** with various bodies involved in the management, control, auditing and investigation of complaints and cases indicating signs of fraud; - **monitoring and analysis of systematic risk**, focusing on declarations for release into free circulation and on the behaviour of economic operators, following the entry into force of legislation on EU trade policy.
RO	Efficient fraud monitoring; development, consolidation and implementation of control and investigation systems. The Paying Agency for Rural Investments (AFIR) and the Payments and Intervention Agency for Agriculture (APIA) have implemented their own anti-fraud strategy for the period 2023-2027. Legislative acts have been adopted: - creating the national regulatory framework for the new 2021-2027 programming period - **strengthening the legal framework** governing conflict-of-interest situations, in light of Article 61 of Regulation (EU, Euratom) 2018/1046 (the Financial Regulation) - approving the national anti-fraud strategy for the protection of the EU's financial interests in Romania, 2023-2027 (Government Decision No 1259/2023). Other measures adopted to lower the incidence of fraud were: - developing operational procedures detailing the measures taken to prevent, detect and penalise fraud, and to recover the damage caused by fraud; - **using risk prevention tools** (e.g. the Arachne and PREVENT IT tools, and cooperation agreements/protocols with the National Intelligence Agency, the Department for the Fight Against Fraud, the National Trade Register Office, etc.) - developing and implementing a robust internal management and control system; - establishing clear **reporting mechanisms**; - developing an ethical and anti-fraud environment through the adoption of the **code of conduct**, which applies to all staff in the management structures and to the beneficiaries; - strengthening the ability of staff in the management and control system to verify the expenditure claimed for reimbursement (e.g. through **instruction/training**) - assessing and monitoring major risks and fraud risks, etc. - implementing the **fraud risk assessment tool** to assess the impact and likelihood of fraud risks occurring within key work processes; - monitoring fraud risks and the action plan, in line with the rules of the programmes;

	- having management structure staff **participate in information and training events** related to: fraud prevention, conflicts of interest, incompatible offices, and integrity; - implementing the '**whistleblowing**' system at institutional level; enhancing beneficiaries' capacity to prepare mature projects and to claim eligible expenditure (e.g. helpdesk, training/guidance).
SE	The incidence of identified fraud is low. In a status report on identified irregularities in 2019, approved in 2021, the Council for the Protection of the EU's Financial Interests in Sweden noted that errors that could also potentially constitute fraud are most likely under-reported and are not notified to the public prosecutor's office. Given the above, the Council for the Protection of the EU's Financial Interests has carried out **training initiatives** aimed at authorities managing EU funds in Sweden and has developed a **notification policy** under which authorities are required to report all irregularities that could objectively constitute attempted fraud. In 2023, the number of reported cases of suspected fraud concerning EU funds received by the Swedish Economic Crime Authority (*Ekobrottsmyndigheten*) increased significantly. The government has also launched an investigation into the effective management of EU funds in Sweden. Amongst other things, the investigation was tasked specifically with examining whether there is a need to **introduce a statutory reporting obligation** for the authorities managing EU funds in Sweden regarding suspected fraud. The investigation report is due to be presented in March 2024.
SI	Reply from the Ministry of Cohesion and Regional Development (MKRR) to question 1.2: Appropriate control system – **both administrative controls and on-the-spot checks**. The managing authority's anti-fraud strategy. Reply to question 1.3: risk analysis in the context of controls or management verifications and, in this context, fraud risk analysis. Reply from the police to question 1.1: For many years, the police have placed a strong emphasis on investigating crimes involving fraud to the detriment of the EU and Slovenia. Otherwise, the police do not have a specific fraud risk analysis for assessing to what extent the low detection rate is due to low levels of actual fraud. In 2016, the police started to monitor and analyse complaints to the prosecution services relating to fraud offences to the detriment of the EU more actively. We estimate that the police dealt with a **relatively small number of such fraud offences** between 2010 and 2023. The monitoring of police complaints made to the prosecution services shows that the relevant supervisory authorities report relatively few instances of abuse to the detriment of the EU's financial interests, but we consider that, given the amount of European funds allocated, the problem in this area is significantly higher than perceived. The police do not have any information as to why this is the case, but would like to

	see more effective detection and reporting of such crimes by the supervisory authorities. To this end, it carries out a number of activities, **such as training and cooperation with supervisory authorities and the EPPO.** Reply from the Financial Administration (FURS) to question 1.2: The Slovenian Financial Administration estimates that the incidence of fraud in the customs area is low, mainly due to **effective risk analysis, including for the protection of EU funds**. When released for free circulation, both national and EU guidance is properly and timely implemented, which has a preventive impact on reducing the incidence of fraud. In addition, a risk analysis selects companies to undergo post-release controls. No additional measures were taken to determine the incidence of fraud.
SK	To judge by the numbers of fraudulent irregularities concerning EU budget expenditure reported by the Member States from 2020 to 2022 (see PIF reports 2020-2022), Slovakia does not have a very low incidence of fraud. Relatively high level of detections can be attributed to the effective functioning of the audit and control systems, to fraud risk assessments and to follow-up on media reports on the possible misuse of EU funds. As regards the revenue side of the EU budget, the identification of VAT fraud is based on the comparison of data from control statements and other available data. Risk profiles are used to identify customs fraud and are based partly on risk identified risk through data analysis methods. However, insufficient capacity does not allow to deal with the entire volume of tax fraud. Prioritising the highest tax risks distributes the risk among multiple entities in lower amounts. Even in cases of identified fraud, effective resolution is not always possible because of ineffective penalty systems and insufficient enforcement of both additional tax and financial penalties. Other problems include limited cooperation between administrative authorities and law enforcement authorities and inadequate legislation on personal data processing, restricting the powers of administrative authorities.

Q.1.3 If YES to Q.1.1. Have you invested in fraud risk analysis to assess the reason for low detection of suspected fraud in your operations?

Among Member States that assess their incidence of fraud as low, almost all (94%) indicate that they have invested in fraud risk analysis to assess the reasons for low detection of suspected fraud in their operations.

Among those Member States that responded to this question, 59% indicate that they have conducted/invested in fraud risk analysis to assess the reason for low detection of suspected fraud in their operations.

	Member State	**TOTAL**
Yes	AT, BE, BG, CZ, DE, EL, ES, FI, HR, HU, LT, LV, MT, NL, PT, SI	16
No	DK	1
n/a	*CY, EE, FR, IE, IT, LU, PL, RO, SE, SK*	*10*

Q.1.4 If YES to Q.1.3. Have you identified weaknesses in fraud detection?

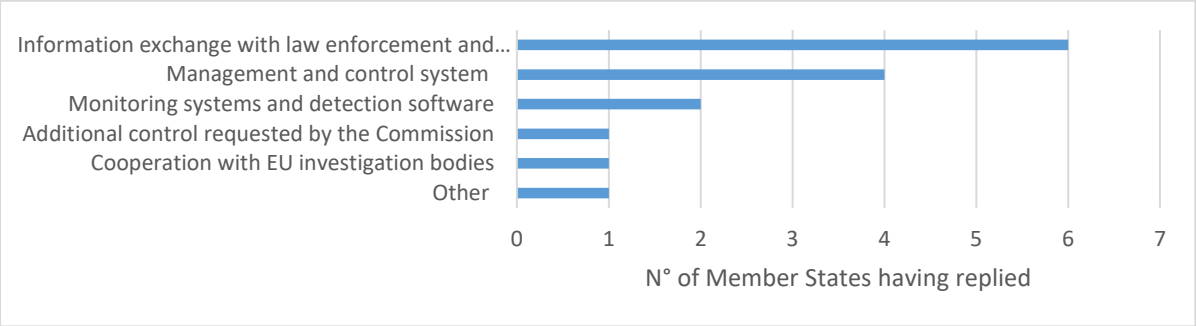
The results from those Member States that have invested in this fraud risk analysis show an equal distribution of cases where weaknesses in fraud was identified.

	Member State	**Total**
Yes	BG, CZ, ES, FI, HR, HU, LT, SI	8
No	AT, BE, DE, EL, LV, MT, NL, PT	8
n/a	*CY, DK, EE, FR, IE, IT, LU, PL, RO, SE, SK*	*11*

Q.1.5 If YES to Q.1.4. In which of the following detection areas have you identified weaknesses?

Most weaknesses identified relate to 'information exchange with law enforcement and specialised agencies'.

Areas of identified weakness	**Member State**	**Total**
Management and control system	CZ, ES, FI,LT	4
Additional control requested by the Commission	ES	1
Monitoring systems and detection software	ES, HR	2
Information exchange with law enforcement and specialised agencies	BG, CZ, ES, HU, IE, SI	6
Cooperation with EU investigation bodies	SI	1
Other controls (please specify)	FI	1



Q.1.6 Usually the issue of intentionality related to an irregularity is investigated in the framework of penal proceedings, with the involvement of criminal law enforcement agencies and public prosecutors. Are there other types of proceedings where intentionality is assessed, in view for example of making a decision about sanctions?

Most Member States (59%) state that there are no other types of proceedings where intentionality was assessed. These instances are detailed in the question below.

	Member State	**Total**
Yes	CZ, EE, EL, ES, HR, HU, LV, PL, SI, SK	10
No	AT, BE, BG, CY, DE, DK, FI, FR, IE, IT, LT, LU MT, NL, RO, SE	16
n/a	PT	1

Q.1.7 If YES to Q.1.6., could you specify what these proceedings are?

MS	Input
CZ	Proceedings in respect of criminal offences under to the Czech Act on Liability for Offences and Procedure thereon (Act No 250/2016 Coll.). Administrative proceedings initiated by tax administrators or administrative authorities for tax or administrative offences.
EE	Estonia uses **criminal proceedings and administrative proceedings** to investigate intentional violations. For example, the **normal administrative procedure is used to investigate** cases like agricultural projects where the support conditions were falsified or documents forged, etc. A lack of resources (people, time, finances, etc.) means that these cases are often not prosecuted, though the funds are generally recovered from the applicants or the support is cancelled. These administrative measures are an easier and quicker way to protect the EU's financial interests. - **Penal and misdemeanour proceedings** regulated in the Estonian Penal Code are used to assess intent regarding revenue.
EL	**Special Service for Institutional Support and Information Systems**: The management and control system (PROCEDURE ΔVIII_2) provides that in an examination of indications of fraud and reporting suspicions of fraud where the outcome of the investigation confirms the suspicion/indication of fraud, then administrative or judicial proceedings must be initiated at national level and the case constitutes a suspicion of fraud. The managing authority then, under the responsibility of the Head of Service, takes the following actions: - sends the investigation team's report and documentation to the National Transparency Authority (NTA)/AFCOS; - sends the investigation team report and the relevant documentation to the Special Service for Institutional Support, the Certifying Authority and EDEL (but not to the beneficiary); - reports the suspected fraud to the EU; - decides on the corrective actions to take (e.g. checks on the beneficiary's other operations, suspension of funding, etc.), based on the type and extent of the suspected fraud; - takes action to prevent such incidents and/or sends proposals for measures of general application to be taken at the level of the management and control system; - informs the Internal Anti-Fraud Network through the managing authority's representative (person responsible for fraud matters). **Recovery and Resilience Facility Coordination Agency:** Irregularities detected in the verifications/controls carried out in accordance with the management and control system of the Greek RRP give rise to penalties. These may be administrative (recommendations from the RRP implementing bodies) or financial (recovery of the irregular funds spent).
ES	The **tax inspection** procedure, on the revenue side. And in general, all

	administrative penalty procedures. Intentionality is assessed to determine the corresponding penalties.
HR	Contribution from the Ministry of Agriculture: Proceedings under the Misdemeanour Act (Official Gazette of the Republic of Croatia) Nos 107/2007, 39/2013, 157/2013, 110/2015, 70/2017, 118/2018, 114/2022); **enquiries and criminal investigations** to ascertain the existence of elements necessary for indictment and launch of criminal proceedings. Contribution from the Customs Administration (Ministry of Finance): In the absence of suspicion of a criminal offence, misdemeanour proceedings are conducted and **a fine is imposed**, the amount of which depends on the seriousness of the offence.
HU	Prior to and in parallel with criminal proceedings conducted by the institutions managing EU funds for the offence of fiscal fraud as defined in Section 396 of Act C of 2012 on the Criminal Code, typically in connection with the use of EU funds, the managing authority concerned **acts on the basis of an irregularity decision**, subject to the proceedings of the other parties, and is entitled to the rights of other parties in the respective criminal proceedings.
LV	Information provided by the Ministry of Agriculture and the Rural Support Service: When applying an administrative penalty, an assessment is done to evaluate whether non-compliance was intentional.Intentional non-compliance can result in exclusion (exclusion from the opportunity to receive EU funding for up to 3 years). The beneficiary is excluded if it is found that: 1) the beneficiary knowingly provided false information; 2) during the implementation of the project, the beneficiary knowingly provided false information to the Rural Support Service or otherwise behaved maliciously in connection with the implementation of the project. Information provided by the Central Finance and Contracting Agency: For violations of procurement norms and other violations not classified under fraud and suspected fraud. Intent and deliberateness are always assessed, including in order to apply proportionate sanctions.
PL	- Intentionality is assessed in proceedings before the Chief Spokesperson for Public Finance Discipline. '**Public finance discipline'** refers to a specific, desirable situation which is achieved through compliance with established legal standards relating to the broadly understood financial economy. An infringement of financial economy rules may result in certain individuals being held liable. This issue is regulated in the **Act on liability for breach of public finance discipline** [*Ustawa o odpowiedzialności za naruszenie dyscypliny finansów publicznych*]. - **The rules on liability** apply to persons who manage public funds inappropriately, e.g. persons who perform functions in entities implementing the budgets or financial plans of entities in the public finance sector, the managers of such entities (e.g. mayors of urban and rural municipalities, chairs of district executive boards, treasurers, heads of schools) or persons required to implement projects co-financed by the EU to whom public funds have been allocated for this purpose or persons who use such funds (in Poland, EU funds are subject to the same rules as national public funds). Penalties for being

	found liable include a formal admonition, a reprimand, a financial penalty, and a temporary ban on exercising functions involving management of public funds.
SI	Ministry of Cohesion and Regional Development (MKRR) The managing authority's 'instructions for carrying out management verifications and verifications of the performance of delegated tasks' (referred to below by their Slovenian abbreviation, **NPO**) set out a **system to deal with ineligible costs and irregularities.** A distinction is made between action taken in the case of management verifications under the responsibility of the body carrying out management verifications and action taken in cases where the body carrying out management verifications reports suspicions of fraud to the competent authority on its own initiative. Fraud is distinguished from the more general concept of 'irregularity' by intentionality. 'Suspected fraud' means an irregularity which requires the appropriate procedure to be launched at national level to determine whether the act was intentional and, in particular, whether there was fraud. - When an irregularity is detected, a correction is imposed if suspected fraud is also detected and a separate declaration is made. If the competent authorities confirm the fraud, they must impose measures and the intermediate body must act in accordance with the provisions of the call or co-financing contract, which require zero tolerance for fraud. A suspicion may also arise if irregularities resulting in the imposition of a correction are not detected. 'Suspected fraud' is defined in the NPO as an irregularity giving rise to the initiation of **administrative and/or judicial** proceedings at national level to establish whether the act was intentional and, in particular, whether it constitutes fraud as defined in Article 1(1)(a) of the Convention on the protection of the European Communities' financial interests. Financial Administration (FURS): This is an offence procedure. Under Article 9 of the Minor Offences Act (ZP-1), anyone who commits an offence, whether through negligence or intent, is liable for the offence.
SK	In Slovakia, intentionality is assessed also in **minor offence proceedings** (Act. No 372/1 990 Coll. on Minor Offences as amended) as well as in penal proceedings. In certain administrative proceedings the administrative authorities assess the gravity of conduct. This can have an impact on the penalty imposed (e.g. in proceedings conducted by the Public Procurement Office or by the Slovak Anti-Monopoly Office).

Q.1.8 In IMS, the Member States must specify the type of proceeding an irregularity is undergoing, choosing among the following options: AP (administrative proceedings), JP (judicial proceedings), PP (penal proceedings). The code PP should be used in relation to suspected fraud, whenever a criminal proceeding is initiated. However, it is possible that the code JP has been used by some Member States for proceedings in relation to suspected fraud, for example when the trial stage is reached. Sometimes, the indication of the code JP is not accompanied by the classification IRQ3. For such cases, to what type of judicial proceedings are you referring?

MS	Input
BE	**ERDF Wallonia**: To judicial proceedings to **recover the irregular amounts**.
BG	- Specified and strictly applied, that 'PP penal proceedings' should always be selected from the 'Type of procedure' field, either singly or in combination with any of the other options. - The option of 'JP judicial proceedings' is **not used for suspected fraud**. It is used only where **administrative cases** have been initiated to challenge decisions by heads of managing authorities determining financial corrections or establishing public state receivables. - The 'JP' option is also used to identify judicial cases initiated to **appeal against enforced recovery of irregular amounts by the authorities of the National Revenue Agency, to identify insolvency proceedings and to identify appeals against decisions refusing verification**.
CY	- To 'JP judicial proceedings' concerning **civil cases for the recovery of unduly spent amounts.**
CZ	- The use of the code JP (judicial proceedings) is usually accompanied by an IRQ3 or IRQ5 classification. Some managing authorities use only the option PP (penal proceedings). The code JP (legal proceedings) combined with the classification IRQ2 would be used when the beneficiary is pursuing in court an unpaid amount which, in their opinion, was not an irregularity.
DE	- Federal State of Baden-Württemberg: no cases of suspected fraud to date, irregularities identified using AP - Hanseatic City of Bremen: not relevant - Federal State of Rhineland-Palatinate (RLP): no such cases in RLP - Federal State of Saxony-Anhalt: action brought by the beneficiary following the granting authority's notice of withdrawal
DK	- The Danish Business Authority replied that in general, they make few reports about irregularities or suspected fraud. However, over the years they have made use of both AP, JP and PP **depending on the case and if it required further investigations by the police or if it resulted in a conviction.** - The Danish Agricultural Agency uses code **JP** if the legal basis of an **administrative decision regarding an irregularity is challenged in court**. - The Danish Fisheries Agency reported the following: 'When we report irregularities, we usually choose 'Administrative Procedure (AP)' rather than legal procedure (JP). In relation to what code we use, we almost always use: If fraud is suspected: (ATBC) Amount must be calculated, After calculation / in

	case of irregularity: (RUNW) Recovery procedure initiated. = Repayment claim has been sent to the beneficiary (FULR) Full Recovery = Beneficiary has paid (AIRR) The amount is irrecoverable (bankruptcy) = Beneficiary is bankrupt (in dividend) **We do not use the code IRQ3.'**
EE	- In Estonia we use codes IRQ3 and AP for administrative but intentional cases.
EL	**Financial Audit Committee:** The option used by management and control system bodies is AP, as financial audits reveal cases of suspected fraud, which are then forwarded to the competent authorities for further investigation. **Ministry of Rural Development and Food:** In court proceedings in which the person concerned uses the legal remedies and remedies provided for in the Code of Administrative Procedure to bring an appeal to the national administrative courts (and, where appropriate, to the Council of State) against administrative acts adversely affecting them, such as decisions to attribute undue payments to him or her. **Recovery and Resilience Facility Coordination Agency:** Regulation 241/2021 does not require Member States to use the Irregularities Management System to report irregularities to the EU. However, an update is emailed to OLAF. To date, no irregularities have been identified that fall within the category of judicial proceedings (JP).
FI	- This refers to cases where the beneficiary appeals against an administrative decision, **leading to court proceedings** before an administrative court.
FR	- The JP (judicial proceedings) code is indicated in the IMS forms when an administrative procedure is brought before the administrative and/or criminal courts.
HR	Contribution from the Ministry of Agriculture: The Paying Agency for Agriculture, Fisheries and Rural Development records cases of suspected fraud in the IMS under Chapter 1.15 using the code JP (judicial proceedings) **where an indictment has been issued as part of criminal proceedings.** The code used for confirmed fraud under Chapter 1.15 is PP (penal procedure), whereas the code used for irregularities is AP (administrative procedure). - Contribution from the Ministry of Agriculture – Directorate of Fisheries: Hitherto, no procedure other than the administrative procedure (AP) has been used under the European Maritime and Fisheries Fund and the European Maritime, Fisheries and Aquaculture Fund.
HU	- The guidelines which the AFCOS developed and made available to the reporting organisations and the material covered in the training courses it regularly organised clearly emphasise that the code PP applies when criminal proceedings have been initiated. Code JP may also be added when other judicial proceedings are ongoing at the same time.
IE	n/a
IT	As regards the use of the **code PP** ('penal proceedings') or **JP** ('judicial proceedings') in **field 1.15** of the IMS form relating to the data to be entered in **field 6.12**, classification **IRQ3 - suspected fraud** (and likewise classification **IRQ5 -**

	established fraud) in field 6.12 must be used only in conjunction with the **code PP**, while the **code JP** (and the **code AP**) can only be used in conjunction with classification **IRQ2** - **non-fraudulent irregularity** for irregularities to be recovered via administrative proceedings (Regional Administrative Courts - TAR), accounting proceedings (accounting courts) or civil proceedings (civil courts). In the initial phase of penal proceedings, the IRQ2 classification may be used in conjunction with the code PP. The managing authority will, however, monitor the status of the proceedings. If the party under investigation is indicted, the IRQ2 classification will be changed to IRQ3. Conversely, the code JP may not be used with the IRQ3 classification.
LT	The code JP (if not accompanied by classification IRQ3) is used for **administrative proceedings, which are carried out in Court** (for example, when the beneficiary appeals the intermediate body's decision on irregularity and the Court has not yet adopted a final decision).
LU	n/a
LV	Information provided by the Ministry of Agriculture and the Rural Support Service: All cases of irregularities are coded AP (administrative proceedings). If an **appeal** against the decision on the recovery of **unreasonably paid funding is brought before the court** - then the code JP (judicial proceedings) is used. Code PP (penal proceedings) is used in cases where a criminal case has been initiated. These codes are not changed even if court proceedings have ended, so they show whether a case has had an appeal, a criminal trial, etc. If these codes were removed after the end of the court proceedings, then when reviewing the case nothing (except the description of irregularities) would indicate that there was a criminal trial or an appeal. Such a case would not be found when entering the code PP (penal proceedings) in the search engine.
NL	Not applicable. The Netherlands has not implemented the IMS but instead applies specific national anti-fraud IT tools.
PL	The use of the 'JP' code in notifications sent by Poland means that proceedings are **pending before an administrative court**, and the case is **classified as an irregularity** (IRQ2).
PT	As a rule, the code JP is also used for situations where **the beneficiary has initiated legal proceedings** because they disagree with the demand to return the amounts resulting from the detected irregularity. In such cases, there are no indications of fraud.
RO	The beneficiary appealing to the administrative court, challenging the debt settlement decision.
SE	n/a - There are no judicial proceedings in this context.
SI	Ministry of Cohesion and Regional Development (MKRR) A reference is used in cases where (different) proceedings are brought within the jurisdiction of the courts, namely: - in cases of an irregularity already reported, an update is subsequently reported due to the opening of bankruptcy or other insolvency proceedings against the beneficiary; these procedures fall within the jurisdiction of the courts; - in cases where the State initiates judicial recovery of funds against the

	beneficiary because the beneficiary does not wish to repay them; and - in cases where legal proceedings are brought by the beneficiary against the State for disagreement with the financial correction imposed.
SK	In Slovakia, the code PP is used for all stages of criminal proceedings, including trial stage. The code JP isused only in relation to irregularities with classification IRQ2. **The code JP is used if civil/administrative court proceedings have been initiated for the recovery of any undue amounts (including enforcement and insolvency proceedings).**

Q.1.9 In your opinion, what are useful elements to formulate the hypothesis that an irregularities might be intentional and consequently suspected fraud worth being further investigated by the competent authorities? (for example, (i) beneficiary or contractor linked to other irregularities or with criminal records, (ii) certain links between beneficiary, contractors, subcontractors, suppliers, (iii) certain inaccuracies or specific elements in certain documents; (iv) certain shortcomings in the implementation of projects, such as the site of the operation cannot be easily found or is clearly inadequate, etc.)

MS	**Input**
AT	- Advantages (e.g. economic) for the beneficiary ---> NB **Case-by-case analysis** essential
BE	- ERDF Wallonia: **Data injection and analysis of risk indicators** provided by **ARACHNE**, recourse to law firms, consultation of national, regional, European registers at our disposal, UBO (ultimate beneficial owner) registry…
BG	The useful aspects to take into account when assessing whether an irregularity might be intentional can be: - **certain shortcomings in the implementation of projects**, for example, the site of the operation cannot be easily found or is clearly inadequate. We have had cases in which the beneficiary or the assets cannot be found at the project implementation address, so further investigation is needed and they are sometimes classified as suspected fraud; - **examination of links** between beneficiary, contractors, subcontractors and suppliers; - beneficiary or contractor linked to other irregularities; - definition of intent; - analysis of how the irregularity arose; - certain shortcomings in the implementation of projects; - users claim partial or complete lack of the provided services, but the documents submitted certify full and high quality service provision; - reasonable suspicions of agreements, decisions or concerted practices between participants, e.g. complementary bidding, participation on a rotating basis, awarding contracts just below the thresholds, etc.
CY	- all of the elements mentioned in the example could be useful to formulate the hypothesis of intentionality
CZ	The irregularity should be considered in the wider context of the whole project: has there been a one-off breach of conditions and rules or is there repeated misconduct. Another important factor is whether or not the beneficiary

	communicates, tries to correct the misconduct or avoids the reported control by providing relevant explanations, etc. Conflicts of interest in public procurement, gross misrepresentation and false data/documents (falsified contracts, rigged or non-transparent tenders and artificial creation of conditions for obtaining subsidies) should also be taken into account. Key is the **intention/motive** to enrich oneself or someone else together with the intention/motive to obtain a financial or material benefit in violation of an obligations laid down by law legal requirements.
DE	- In the case of ERDF funding in Baden-Württemberg, for example, the original project documents can be used to determine the legality of the **conditions for allocating public funds** to the funding case. In addition, the supporting documents can be checked for authenticity. Moreover, payments are corroborated with copies of proofs of payment, which are checked for consistency against the original during the on-the-spot inspection. If documents have been forged or falsified, these activities are covered by the above-mentioned legislation on fraud, subsidy fraud and forgery. To date, no **falsification of supporting documents** has been found in the cases examined. - By concentrating all cases supported by the European Regional Development Fund with *L-Bank,* and through the unified customer database in *L-Bank*'s overall database, along with the sufficient array of additional *Land* and federal funding for *L-Bank*, systematic cross-checks ensure a clear overview of the beneficiaries. Unreliable beneficiaries can then be excluded from funding where such cases are found. Hanseatic City of Bremen (ERDF): - **Training to raise staff awareness of signs of a possible case of suspected fraud**. The professional experience of staff is also a key aspect when assessing irregularities. Federal State of Rhineland-Palatinate: **A case-by-case examination i**s carried out. Federal State of Saxony-Anhalt (ERDF): - links to other irregularities - links between beneficiaries (e.g. affiliated undertakings), conflicting information
DK	- Danish Business Authority: elements in certain documents that raise suspicion e.g.. **use of the same words/phrases/spelling mistakes etc**. - Danish Agricultural Agency: cases with red flags indicating that documents may have been manipulated. - The Danish Fisheries Agency: whether the beneficiary has already been reported in other cases; whether the beneficiary is admissible; the process as a whole (i.e. if the vessel is sold immediately after payment). A post-check of admissibility is also carried out.
EE	Any details that are in doubt should be investigated, not just those listed in the question. We use a **system of red flags** and have produced appropriate

	guidance. This helps the authorities to detect intentional infringements and prove them in administrative proceedings. Also, more experienced colleagues advise and help the officials conducting the grant application procedure to solve complex cases.
EL	**Special Service for Institutional Support and Information Systems:** a. beneficiary or contractor linked to other irregularities or to criminal records; b. certain links between beneficiaries, contractors, subcontractors and suppliers
ES	- a history of administrative or criminal infringements committed in the past by a beneficiary or by a contractor; - œrtain links between **beneficiaries, contractors, subcontractors and supplier**s; - whether the beneficiary has recently worked in a management position in a company applying for EU funding; - inaccuracies or specific items in certain documents; - **falsification of documents**; - similarity in the format and content of documents provided by different contractors for the same public procurement procedure, or by several beneficiaries for the same call for competitive grants; - procedural irregularities in the processing of the file concerned; - irregularities in the supporting documents provided by the recipients of the funds; - certain deficiencies in the implementation of projects; obvious inappropriateness of the location of the operation, or difficulty in identifying the location of the operation; - disappearance of the investment; - verification of a change or diversion of the subsidised activity; - non-existence of the project after verification during the on-the-spot check; - projects with very significant amendments that prevent the fulfilment of the project's purposes; - the **existence of a** friendship, personal relationship or family relationship between a contractor or beneficiary and a public employee involved in the administrative procedure and who has not abstained from that involvement; - creation of artificial conditions for obtaining the aid, etc.
FI	The pre-trial investigation authorities in charge of the criminal investigation assess the intentional nature of the act and the constituent elements of the criminal offence.
FR	Links between the aid beneficiary and the suppliers; Forgery of documents (undated contracts, forged invoice dates) to ensure that the application artificially meets the conditions for access to aid with fraudulent intent.
HR	*Contribution from the Ministry of Regional Development and EU funds:* All of the examples given in the question could prove useful with regard to the

	European cohesion policy. *Contribution from the Ministry of Agriculture:* **Forged paperwork** - Physical aspect: if a document is physically altered, e.g. by striking through points or instructions or adding information manually - Substantive aspect: if the content of a document is at odds with the actual situation, e.g. a false description of a service rendered, fictitious content, forged signatures, etc. **Artificial creation of conditions** - Division of a business entity or partitioning of a project, i.e. a functional, financial and technological whole, into two or more parts - Links (personal, property, economic) between suppliers under the same project - Links (technical, technological or economic) between two or more business entities or holdings, in terms of partnership and capital, agricultural activity per entity - Owners/managers in associated companies related through marriage or blood. **Conflict of interest** - Links between the beneficiary, contractor, subcontractor and supplier. *Contribution from the Ministry of Agriculture – Directorate of Fisheries:* Examples (i) and (ii) should definitely be taken into account when assessing whether an irregularity is intentional, i.e. whether it contains elements of suspected intentional conduct. Implementation of the contract must also be considered; this is verified through an on-the-spot check at the beneficiary's facility (e.g. obvious tampering with the serial number on newly purchased equipment, or with construction log books, etc.). *Contribution from the Croatian AFCOS:* **Purchase of second-hand rather than new equipment**, such as: - components of a plant incorporating items that were manufactured long before the date of the equipment purchase contract between the beneficiary and the supplier (checked by running manufacturer serial numbers through publicly available search engines, comparing serial numbers with those referenced on invoices, checking identification markings on machinery/equipment components); - visible damage to and usage marks on components of machinery/equipment (ashes, corrosion). **The beneficiary's founder and procurator convicted of a crime by a final judgment in another country.** **Inconsistency between invoices.** For example:

	- the invoice and delivery dates on the invoices supplied with the payment claims differ from the ones discovered on the invoice recovered from the beneficiary during an on-the-spot check; - late delivery of paperwork that had previously been declared as non-existent or was not found at the beneficiary's premises; - warranty certificate has the same date as the invoice, yet the equipment model listed in the warranty certificate is not the same.
HU	The organisations that identify irregularities use a wide range of criteria to assess cases of suspected fraud. The specific set of criteria relevant to a particular case is also influenced by the objectives of the project and the nature of the irregularity in question. In some areas, due to **the use of the ARACHNE risk management system,** some elements of suspected fraud can be detected at the first level of control. In addition to the examples given in the question, the criteria considered may include: - conflicting beneficiary declarations; - inconsistencies in the supporting documents; - inaccurate invoices; - false data; - ownership problems; - feasibility of performance; - links with other projects (e.g. double funding); - problems with suppliers (e.g. newly established company). As a general rule, if the elements constituting the relevant criminal offences as defined in the Criminal Code are suspected, the case is referred to the competent investigating authorities to establish the existence of fraud.
IE	• Beneficiary or contractor linked to other irregularities • Links between beneficiaries/contractors/suppliers • Gaps in processes such as permissions around spend approval • Undisclosed conflicts of interest • Changes in procurement mid-process • Splitting of works into below threshold calls for tender • Leaking bid data • Phantom tenderers
IT	In the Italian legal system, only the judicial authority can assess whether an irregularity is intentional. Successive EU regulations have established that the obligation to report a case in the IMS system is linked to '**the primary administrative or judicial finding, understood as the first written assessment made by a competent administrative or judicial authority**', on the basis of a full investigation which, relying on '**actual**' or '**specific**' facts, concludes that an irregularity or fraud has been committed. This conclusion may subsequently have to be adjusted or withdrawn as a result of developments in the course of the administrative or judicial procedure.

As provided by the OLAF **Handbook** on '**Reporting of Irregularities in Shared Management**', 2017 edition, paragraph 6.2., '[t]he final decision on whether an irregularity actually constitutes fraud is the responsibility of the relevant authorities of the Member State involved'. Paragraph 6.3. of the Handbook states that, '[i]f […] a guilty verdict is pronounced and is not appealed against, the case can be considered 'established fraud'.

With regard to the precise identification, according to national legislation, of the '***primary judicial finding***' classifying an irregularity as fraud or, at least, as suspected fraud, the Committee for combating fraud against the European Union had requested a qualified **opinion from the Ministry of Justice** which, in summary, replied as follows:
'…the definition of judicial finding is highly conventional, since EU legislation, albeit of immediate applicability and direct effect, does not aim to harmonise national legislations and is intended to be implemented in States with profoundly different legal traditions. Thus, this definition must be adapted to the domestic regulatory context.'

Having said that, it is necessary to steer away from two extreme positions:
'On the one hand, the obligation to report cannot certainly arise at the time of the initial record of irregularity, even if drawn up by judicial police officers under Article 13 of Law No 689 of 1981' (which is a mere record of initial findings) inasmuch as such record has 'a merely fact-finding value and does not imply any assessment by an authority having decision-making powers (even provisional) in the context of that procedure.'

On the other hand, the primary judicial finding cannot be a finding 'having the force of *res judicata*, which comes at the final conclusion of the judicial proceedings, if only because [the EU regulations themselves refer to] even mere suspicions of fraud.'

Consequently, the '**primary judicial finding**' giving rise to the obligation to report a '**suspected fraud**' must be identified as that occurring 'at the time when the prosecuting judicial authority, ruling out the possibility of closing the case and deciding instead to launch a criminal action, formulates the charge and thus makes the first written assessment of irregularity having some form of stability'. Hence, this primary finding takes the form, 'in ordinary proceedings, of the request for committal for trial or alternative proceedings under Article 405 of the Code of Criminal Procedure', and 'in proceedings before a single-judge court, in which the public prosecutor issues the direct summons to trial, the decree for summons under Articles 550 and 552 of the Code of Criminal Procedure.'

This is because the option under point (c) 'allows the necessary appropriate preliminary examination of the actual criminal relevance of the conduct and safeguards the confidentiality of the investigation' and, moreover, 'it appears to be correct also in a systemic sense, as it establishes a similar mechanism to

	Article 129(3) of the Rules Implementing the Code of Criminal Procedure, which governs the management of information on criminal prosecution in the case of offences that have caused damage to the Treasury, which can include actions against the EU budget.' However, if the misappropriation or wrongful retention of EU subsidies involves persons holding public office, 'it is appropriate to consider as primary judicial finding any arrest, detention or precautionary detention measures issued against such persons, given the grave impact of the unlawful conduct on the system of public offices in charge of managing administrative control procedures, in accordance with the applicable provisions' of the national legislation on the disclosure to be made to the authority for which the public employee works. The Ministry's guidance was subsequently included in the **Guidelines on reporting to the European Commission irregularities and fraud against the EU budget**, approved by a resolution of the Committee for combating fraud against the European Union on 8 October 2019. As is known, the Guidelines currently provide that irregular conduct may be classified as: - '**suspected fraud**' (**code IRQ3**), in the cases referred to in points (c) and (e) above; or - '**established fraud**' (**code IRQ5**) if a criminal court delivers a guilty verdict against a beneficiary and the decision is not appealed (or cannot be appealed further).Code IRQ3 is retained in cases of appeals against a first instance judgment or appeal judgment. In this context, when an authority enters in the IMS system an irregularity that has been reported to the criminal judiciary - even just via a complaint or a *notitia criminis* - it must (a) report the existence of penal proceedings by inputting the code PP in the form to be submitted on the IMS (unless confidentiality demands otherwise) and (b) constantly monitor how the competent judicial office's penal proceedings are progressing, so that the main code can be promptly changed from 'irregularity' to 'suspected fraud' as soon as the investigated parties are indicted or the other above-mentioned conditions occur. The Committee regularly highlights these requirements as part of the continuing guidance and support it provides to all managing authorities in Italy. The Committee stresses the need to keep carefully monitoring cases entered in the IMS that are known to have been reported to the judicial authority, including those closed due to decertification or total recovery. This monitoring activity could also be facilitated by the full entry into operation of the EPPO, which has competence over all investigations into any type of offence concerning EU funds above EUR 10 000 committed after 20 November 2017 (largely coinciding with all the cases of fraud against the EU budget, to be entered in the IMS).Concentrating these investigations in a few judicial offices, i.e. those involving European Delegated Prosecutors, could streamline the communication flow between the managing authorities and the judicial

	authorities. In any event, the national orientation whereby fraud is classified as such at the time of committal for trial seems to be firmly established at present. It is fully consistent with the applicable EU rules and makes it possible to describe the fraud on the basis of actual and specific facts, as required by the regulations, while avoiding ascribing criminal liability to individuals without proper judicial review. Furthermore, the competent national authority considers this criterion to be systematically coordinated with other procedural rules governing the external reporting of facts that give rise to an offence. The Financial Police have found that, when assessing whether an irregularity might be intentional and so constitute suspected fraud requiring further investigation, previous administrative inspections provide can provide useful indications of fraud in thefields of **taxation** and **public expenditure** among others. The discovery of **invoices or other documents relating to objectively or subjectively non-existent transactions** is an aspect that can objectively justify the sending of a *notitia criminis* to the competent judicial authority. Other aspects to be taken into account in assessing whether an irregularity may be intentional are: in **procurement**: - tenders with blatantly unjustified limitations to access, or poor quality of tender documentation and specifications, as well as lack of transparency in the assessment process and deficiencies in execution; - existence of personal relationships between tender officials and economic operators which can be easily exploited for fraudulent purposes, taking into account the actual ownership of the relationships; - existence of business networks, corporations, possible shell companies for submitting multiple funding applications, controlling the project supply chain, concealing beneficial ownership or building artificially long supply chains; in **applications for incentives/funding/contributions**: - incomplete information or missing or inaccurate supporting documents; - ineligible expenditure due to failure to comply with requirements; - incorrect application of reporting rules, failure to meet deadlines; with regard to **traditional own resources:** - evidence of under-invoicing on imports; - false documentation attesting the release for consumption of products; - incorrect classification of goods, especially as regards their origin; with regard to the **area-related aid schemes in the agricultural sector:** - evidence that the titles attesting to the ownership or tenure of the land benefiting from the premium are false.
LT	When assessing whether the violation could be intentional, one must look at all

	the actual circumstances that could testify to it, including the circumstances exemplified in the question, as well as, for example: the creation of artificial conditions; actions performed in a conflict-of-interest situation; deliberate actions of the funding beneficiary in continuing to implement the projects with potential infringements of or non-compliance with project implementation rules; the fact that beneficiary has previously been penalised for infringements in a specific field or industry. The guidelines developed by AFCOS 'Criminal offences against the EU's financial interests: definitions, typologies, characteristics and examples of practice' are applied.
LU	n/a
LV	Mainly beneficiary or contractor having links to other irregularities or having criminal records, or certain links between beneficiary, contractors, subcontractors, suppliers
MT	**Having a thorough understanding of the project and experience in EU funding** are considered two key aspects when assessing whether irregularities warrant further investigation. A comprehensive grasp of the project's intricacies and the progress of the project activities can help in determining if anomalies or irregularities observed demand a more in-depth examination. The standard operating procedure on checks and verifications to be carried out by managing authorities on conflict of interest and ultimate beneficial owners for EU-funded contracts includes a **risk assessment checklist.** Contracts that exceed a certain score will be subject to a detailed check. The risk factors covered in this checklist include situations where: the same contractor is granted multiple contracts by the same beneficiary; a single bid is received for a procurement process; a contract is awarded by a direct award, and a contract with a long term duration is awarded. The Public Procurement Directives also contain measures directly enhancing transparency and tackling corruption. For instance, as the post-award period is particularly vulnerable to corruption, **the rules for changing contracts during their term have been clarified to remove any doubts.** To gain insight into the intention of a suspected fraudster, it is useful to assess whether the **fraud triangle factors (pressure, opportunity and rationalisation)** are present **(along with capability)**. For example, a suspect living beyond their means would be an indicator that their actions potentially constituted not merely an irregularity but fraud.
NL	In evaluating the intentionality behind irregularities, the Netherlands applies the EU definition in Directive (EU) 2017/1371. Examples of indications considered intentional are**: falsification of documents, identity fraud, duplicate payment requests, claimed construction activities which cannot be traced during on-site visits, clearly intentional omission of information, links with criminal organisations, indications of collusion between organisations or natural persons**.
PL	Article 304(2) of the Code of Criminal Procedure requires national and local government institutions in Poland to report an offence prosecuted *ex officio* (where the institution has become aware of such an offence in connection with

	its activities) to a law enforcement authority (public prosecutor, the police or another body authorised to conduct investigations). Based on the offence reported, the competent authorities who have received the report may decide to initiate an investigation. When reporting an offence, an institution must provide evidence to substantiate its suspicion that an offence has indeed been committed. To do so, an institution may conduct its own investigation, taking into account various aspects, such as **personal links with the project, implementation or involvement in the implementation of a significant number of contracts and projects, previously detected irregularities involving specific entities/persons, ongoing proceedings in respect of the projects/entities concerned**. In the field of agriculture, the paying agency now has a list of signs of fraud to **raise awareness** among its employees at all stages of the administrative and control cycle of anomalies (signs) that could warrant suspicion of fraud and to increase the effectiveness of fraud prevention and detection. The list of signs of fraud is non-exhaustive and serves as a basis for further analysis of the applicants' possible fraudulent conduct. It is updated based on the results of the fraud analysis carried out, the results of audits and checks conducted at the agency and findings of the reports and analyses sent by the Commission. Where there are signs of fraud, checks are performed in order to unequivocally confirm or dismiss the possibility of fraud. The activities performed as part of such checks depend on the nature of the warning sign and may include, for example, **cross-checks, verification of the document issuer's data, enquiries/telephone interviews with the issuers of the contested documents, on-the-spot visits/inspections**
PT	- **links between** the beneficiary, contractors, subcontractors and suppliers; - **incomplete documents** or documents with crossings out; - supporting documents for expenditure (invoices) that are not recorded for accounting purposes or not declared to the Tax Authority; - a vague description of the invoiced goods and/or services; - **the same supplier** is repeatedly awarded the tender; - the beneficiary has a history of irregularities and/or debts; - the expenditure presented does not tally with the expenditure actually incurred.
RO	In accordance with Annex 1 to Government Decision No 875/2011 approving the Implementing Rules for Government Emergency Order No 66/2011 on preventing, detecting and sanctioning irregularities in obtaining and using European funds and/or related national public funds, the aspects (factors) to be taken into account when assessing whether an irregularity could be intentional are the relevant fraud indicators (warning signs) for public contracts and procurement, relating to 16 common and recurrent fraud schemes. Other aspects mentioned by the managing authorities are: - the **documentation submitted** by the beneficiary at all stages of the

	project's implementation, (for example: self-declaration, including financial statements and other supporting documents); - the audit bodies' findings regarding aspects involved in the implementation of the projects carried out by the beneficiaries; - checks carried out on the basis of **cooperation protocols** concluded by MIPE with other institutions/relevant bodies (checks using the ARACHNE and PREVENT IT systems); - correspondence between the activities carried out and the supporting documents that the beneficiary submits at all stages of the project's implementation, such as self-declaration, financial statements and the documents included in procurement procedure files. For the RRF, checks are carried out under Government Emergency Order No 70/2022, regarding the prevention, verification and detection of irregularities/double funding, and serious irregularities found in obtaining and using external grants and loans allocated to Romania through the RRF. These checks address all aspects that may give rise to suspected fraud, such as: - **certain links between the beneficiary, contractors, subcontractors and suppliers;** - **beneficiaries or contractors linked to other irregularities or with criminal records;** - **certain inaccuracies or specific elements in certain documents.**
SE	It is not possible to give a brief answer to this question. Each individual notification must be **assessed and evaluated on the basis of what can be proven in the individual case.** It is a complex and qualified assessment that cannot be described in this context. The ERDF managing authority may serve as an example. The authority can see whether the beneficiary has been the subject of any recoveries in current or previous cases, and the reasons for the recoveries of the respective aid processed by the authority in their administration system. This can be an indication of fraud. Conflicts of interest and other links between beneficiaries, suppliers and subcontractors can also be an indication of fraud. Furthermore, circumstances that come to light surrounding irregularities can be an indication of fraud. Finally, shortcomings in implementation can be an indication of fraud. The assessment of intent is ultimately a matter for the police and/or the public prosecutor's office.
SI	Ministry of Cohesion and Regional Development (MKRR) Those doing management verifications must pay attention in their work to the '**fraud warning signs' or 'fraud flags'**, that indicate potential fraud, corruption, etc. The managing authority's 'instructions for carrying out management verifications and verifications of the performance of delegated tasks' contains a list of **fraud red flags** and a reference to additional, extended checking or cross-checking where there is deviation from normal practice. (Detailed in Chapter 6.4 'Fraud indicators' of the Slovenian managing authority's instructions for the implementation of management verifications for the programming period). Slovenian police

	Factors that should be taken into account when assessing whether an irregularity could constitute a suspicion of fraud and should be further investigated are, for example: - insufficient or unclear description of goods or services; - missing supporting documents or certificates relating to eligibility requirements; - non-disclosure of certain evidence; - long response to a request for additional information or completion of the application; - freshly painted machinery or other equipment for an on-site visit; - a recently established company; - the legal entity is not registered in the commercial register, does not carry out the required activity or has recently registered it, does not advertise its activity, does not have its own website, has no references; - family-linked enterprises; family or business links between civil servants (members of the evaluation committees) and of the call participants, subcontractors or suppliers; - a rapid increase in turnover in a very short period of time soon after the business starts operating; - the company's head office is at a residential address; - the beneficiary, external contractor or subcontractor is established at the same address; - similar signatures on attendance lists and others.
SK	- **certain links between beneficiary, contractors and subcontractors; undisclosed conflict of interest;** - **unusual bidding patterns** (e.g. the bids are an exact percentage apart, winning bid just under threshold of acceptable prices or exactly at budget price, incomplete bids, the same shortcomings in different bids, etc.); - other apparent connections between bidders, e.g. same time and place of submission of the bids, etc.; - potential qualified contractors fail to bid and become subcontractors or low bidder withdraws and becomes a subcontractor; - fictitious bidders; - some items for bids different from the actual contract, etc.; - **certain links** between beneficiaries with similar projects activities under the same call for proposal; - certain **inaccuracies or specific items in certain documents**; e.g. inappropriately reported accounts, multiple invoices with the same amount, invoice number, date; - undocumented changes in contracts, apparent irregularities in time sheets (e.g. time taken to move from one place to another is unrealistic), incomplete time sheets, etc.; - certain **shortcomings in the implementation of projects**: excessive quantity of purchases; purchases not consistent with the goals of the project; acceptance of low quality of goods and services; service provider cannot be found in any directories or online etc.;

	- overpaying for purchases – **unwarrantedly high prices**; - the recipient/project has already been **sanctioned in the past** or is subject of proceedings by lawenforcement authorities; as regards VAT fraud: previous circumvention of legal regulations, various links between tax entities, no real business activity, etc.

Q.1.10 Have the bodies in charge of detecting irregularities adequate access to information to assess these elements and consequently to assess the possibility of intentionality?

Nearly all Member States (85%) declared that the bodies in charge of detecting irregularities have adequate access to information to assess these elements and consequently to assess the possibility of intentionality.

	Member State	**TOTAL**
Yes	BE, BG, CY, CZ, DE, DK[20],EL[21] ES, FI, FR, HR, HU, IE[22], IT, LT, LU, MT, NL, PL, PT, RO, SI, SK	23
No	AT, EE, LV	3
n/a	SE	1

Q.1.11 Have you identified weaknesses in your reporting practices for a timely and exhaustive reporting in IMS of suspected fraud cases?

Most Member States (70.4%) have not experienced weaknesses in their reporting practices for a timely and exhaustive reporting in IMS of suspected fraud cases.

	Member State	**TOTAL**
Yes	BG, CZ, EE, EL, ES, IT, LV, SI	8
No	AT, BE, CY, DE, DK, FI, FR, HR, HU, IE, LT, LU, MT, NL, PL, PT, RO, SE, SK	19

Q.1.12 Which measures have been adopted to correct the identified issues?

MS	**Input**
BG	The AFCOS Directorate has issued **Methodological guidelines for irregularity management procedures**; The AFCOS Directorate gives comments and opinions by telephone or email regarding the correct managing of the irregularities; The AFCOS Directorate **checks the information reported in the IMS**; The AFCOS Directorate conducts **administrative control checks** within the managing authorities to identify infringements against procedures for irregularity management. Recommendations are made in case of detection of omission.

[20] Yes, enough to handle administrative proceedings. However, administrative proceedings have their limitations, and it is therefore essential that, when for further judicial investigations are deemed necessary, the police have access to other means.
The Danish Agricultural Agency: The paying agencies in Denmark do not have the authority, competences and resources to investigate and question the parties in suspected fraud cases.
The Danish Fisheries Agency: No. It is the police who investigate and assess whether there is intent in connection with irregularities.

[21] **Financial Audit Committee:** Yes, the management and control system bodies, including the audit authority for co-financed programmes and the supreme national audit body (EDEL), have access to information that could trigger suspicions of fraud. As mentioned above, from their audits the MCS bodies can only establish a suspicion of fraud.

Special Service for Institutional Support and Information Systems: The managing authorities responsible for detecting irregularities in co-financed projects exchange relevant information through the the DIAVLOS internal anti-fraud network platform, to which the anti-fraud officer in each MA has access.

[22] Specific training for intermediate bodies planned.

	The AFCOS Directorate sends the AFCOS Council its **analysis of the findings of the administrative control checks**, which includes proposals for taking adequate measures to eliminate the identified weaknesses in the functioning of the system and prevent those weaknesses recurring in the future. A **permanent working group** has been formed for discussing problems and cases related to the managing of the irregularities. The AFCOS Directorate organises **training for irregularity officers** on the topics related to the IMS usage and on managing irregularities.
CZ	On the revenue side, the **level and platform of communication** between the tax administration and law enforcement authorities now takes place at a higher level.
EE	Delays in reporting suspected fraud are generally related to criminal investigations when the EPPO or other prosecutors are not permitted to report the case**. We still hope that OLAF will make it possible for the EPPO to share investigation information with Member States' authorities.**
EL	**Financial Audit Committee:** The large number of fields to be filled in per irregularity/suspected fraud case in IMS, their complexity and the dual interpretation of some fields, often leads to difficulties in reporting irregularity/suspected fraud cases to OLAF. However, despite these difficulties, the MCS bodies notify OLAF, via IMS, of all cases of irregularities/suspicions of fraud detected during their audits. The Greek authorities have often reported the difficulties mentioned above – in meetings with OLAF on reporting analysis issues and at annual coordination meetings of the audit authority (EDEL) with OLAF and other EU services and in connection with evaluations of the IMS system. The main concern of the EDEL and the other MCS bodies is to address the difficulties. Their hope is that OLAF's requirements for registration in IMS will be simplified as far as possible.
ES	The shortcomings identified are not general, they are limited to the reporting by some specific operational programmes/authorities and concern reporting of all kind of irregularities, not only those relating to suspected fraud. Steps are being taken to **ensure that all outstanding notifications can be submitted.** According to information provided by one of the authorities concerned, the exchange file for uploading irregularities for 2014-2020 to IMS is in production, pending testing to ensure that the notifications are correct, complete and reliable. Ten cases of suspected fraud were reported in the third quarter of 2023.
IT	See Italy's reply to question 1.9. regarding the need for the reporting authorities to **continuously monitor developments** in criminal proceedings and the initiatives taken in this regard.
LV	If necessary, but not less than once a year, letters are sent to law enforcement authorities with a request to provide information on the progress of criminal proceedings.
SE	**Ongoing dialogue between notifying authorities and the public prosecutor's office** when notifications are received.

SI	Ministry of Cohesion and Regional Development Persons carrying out management verifications **have access to the information system of the managing authorit**y containing payment claims with supporting documents from the beneficiary and other documentation relating to the operation checked. They can also check the information using the internet, the public procurement portal, **Arachne, GVIN, AJPES or other data-mining tools** adopted at national level. Measures to correct weaknesses: **Improving administrative checks and updating checklists with cross-checks.**

Q.1.13 If YES to Q.1.11. Which of the following areas did you encounter difficulties in?

Member States which have experienced difficulties in reporting practices for a timely and exhaustive reporting in IMS of suspected fraud cases, predominantly struggle with the following issues. Providing high-quality, complete data in fraud reporting is considered the biggest challenge.

Difficulties in reporting practices	**Member State**	**Total**
Reporting fraud in a timely manner	CZ, ES, LV, SI	4
Reporting all cases of suspected fraud	LV, SI	2
Providing quality and completeness of data in fraud reporting	BG, EL, IT,LV, LT	5
Other (specify)	BG, LV, NL	3

Q.1.14 For each marked answer in Q.1.13. Can you provide an explanation of the reason behind your difficulties?

MS	**Input**
BG	Some of the difficulties identified are due to a **lack of information on the status of judicial proceedings** initiated in relation to the cases of irregularities concerned. There are **no clear guidelines** for the Member States on which stage the irregularity should be reported as suspected fraud at –the stage of the primary administrative or judicial finding, pre-trial proceedings, criminal proceedings or once an indictment is filed. This leads to different practices and affects the number of reported cases. Practices need to be aligned in order to obtain reliable information on suspected fraud cases. Joint meetings and training sessions are also needed. The national competent authorities have not identified weaknesses specifically for suspected fraud, but for irregularities generally. Some of the weaknesses identified are explained below:

	- The method of entering financial information about irregularities in IMS does not comply with Article 4 of Regulation (EU) 2015/1974 under which amounts reported by Member States must be denominated in euro. Financial information about irregularities being investigated is entered in IMS in Bulgarian lev (BGN). - A discrepancy was found in the information entered in UMIS and IMS. - The IMS irregularity reports do not include information about financial operators who, through their actions or omissions, have committed infringements of EU law or related national law. - The IMS irregularity reports do not include information about judicial cases initiated in relation to cases of irregularities being examined. - Information about the full recovery of irregular amounts is not included in the IMS irregularity report, but is reported only at national level in UMIS. - Information about enforcement proceedings initiated in relation to cases of irregularities being examined is not included in the IMS irregularity report. - The changed legal classification of the infringement identified is not reported either at national level in UMIS or to OLAF in IMS.
CZ	Seeking to end tax proceedings first at the expense of timeliness of notification of active infringements.
EL	**Financial Audit Committee:** As mentioned in our reply to question1.12, the large number of fields to be filled in per irregularity/suspected fraud case in IMS, their complexity and the dual interpretation of some fields, often lead to difficulties in the complete and qualitative reporting of irregularity/suspected fraud cases to OLAF.
ES	According to the information provided by the managing authority for the 2014-2020 ERDF operational programmes, the main difficulty they have faced is that **resources are scarce** and had to be devoted to implementing other developments (arising from regulatory amendments) and to developing the Funds 21-27 application. This delay does not entail a problem in the fraud detection capacity of the management and control systems, as the irregularities detected are in the computerised management system for these operational programmes, Funds 2020.
IT	See Italy's reply to question 1.17.
LV	**Not all information about criminal cases not initiated by the EU funds authority is always initially available**. Sometimes there are problems with receiving updated information from law enforcement authorities, as information in criminal proceedings cannot be openly shared. There can be a failure to provide information, due to long deadlines for criminal proceedings. When a large number of irregularities are reported, quarterly contact with the specific investigator is required to clarify progress. This takes away lot of the institution's capacity to perform its basic functions. Also the purpose and meaning of IMS is not fully understood, except for the statistical function. Data entry is very time-consuming, and adds no value in return (in terms of results or further action). Statistics could be provided by linking IT systems without physical data entry.
SI	Ministry of Cohesion and Regional Development Human factors, different understanding/interpretation of which stage to report

	suspected fraud at.

Q.1.15 Have you encountered any difficulties in providing follow-up for investigated fraud cases?

There is a relatively even distribution among the Member States participating in the survey that indicated that they encountered difficulties in providing follow-up for investigated fraud cases.

	Member State	**Total**
Yes	BG, CY, CZ, DK, EL, HR, HU, IT, LV, PL, SE, SI, SK	13
No	AT, BE, DE, EE, ES, FI, FR, IE, LU, LT, MT, NL, PT, RO	14

Q.1.16 If YES to Q.1.15. Has the information flow between judicial and reporting authorities improved?

From the Member States who experienced difficulties in providing follow-up for investigated fraud cases, the majority (69%) state that the information flow between judicial and reporting authorities has partly improved, while the remaining Member States believe that this is not the case.

Improvement information flow	**Member State**	**Total**
Yes, fully	CZ	1
Yes, partly	BG, DK, EL, HU, IT, LV, PL, SE, SK	9
No	CY, HR, SI	3
n/a	*AT, BE, DE, EE, ES, FI, FR, IE, LU, LT, MT, NL, PT, RO*	*14*

Q.1.17 If YES to Q.1.16. What measures have been taken to increase the exchange of information?

MS	**Input**
BG	In case of judicial proceedings, the **methodological guidelines** for managing irregularities under the EU funds issued by the AFCOS in November 2023 give grounds for closing irregularities. The irregularity officers may ask the Prosecutor's Office for information on the progress of inspections and investigations in pre-trial proceedings. The AFCOS Directorate organises **round tables** and **working groups** with representatives of the Bulgarian competent authorities, the Ministry of Interior and the Bulgarian Prosecutor's Office. Within the Bulgarian Prosecutor's Office, a specialised department at the highest level – the Supreme Prosecutor's Office – has been set up and works in close cooperation with the AFCOS Directorate. There is a constant and effective electronic exchange of information, which ensures immediate responses in case of emergencies
CZ	On the revenue side: Systemic use of the Tax Cobra method of work (a joint team of relevant authorities, in which there is an operational **exchange of information and coordination** of individual proceedings).The primary objective is protecting

	the national budget.
DK	Most of the contributions to the survey answered 'No' to Q.1.15. The Danish Agricultural Agency answered 'Yes' to Q.1.15. It reported that communication between the two authorities has improved through meetings and clearer instructions when handing over cases.
EL	**National Transparency Authority (NTA)/AFCOS:** **The Management and Control** System of the National Strategic Reference Framework 2021-2027 and, in particular, paragraph 4.5 ('Follow-up of progress in the investigation of complaints') of Procedure ΔVIII_3 ('Reception and examination of complaints') provides as follows: 'The bodies responsible for investigating complaints (NTA/AFCOS, EDEL, managing authority) must ensure that the investigative work is completed as soon as possible and that the Financial Management and Control authority/AFCOS is informed, with a copy to the Special Service for Institutional Support, the certifying authority and EDEL of the outcome of the investigation.' 'As the national reception point for all complaints relating to co-financed projects, the NTA/AFCOS is responsible for recording the progress of investigating complaints in a single file (complaints table). It uploads this file with the information communicated to it by the investigating bodies on the NTA networking platform. Users can be accredited for this platform by EDEL, the Special Service for Institutional Support and the Certifying Authority, with the necessary safeguard clauses containing sensitive personal data. Once the NTA has posted the complaints table, the EDEL adds the data on the investigation of complaints by its services and the CA then adds data on expenditure and exceptions for projects. This table is kept as a supporting element for submitting the assurance package to the EU.' 'On the basis of the data in the table and in order to determine the amounts of expenditure to be declared to the Commission, the CA may send requests to the bodies investigating complaints (NTA, EDEL, MA) for information and speeding up the investigation procedures throughout the year. 'In order to form an informed view and take decisions within the Accounts by CA and EDEL, all the updated data relating to the investigation of complaints should be available.' In this context, the NTA/AFCOS asks the judicial authorities for an update on the progress of the complaints at regular intervals (approximately every 6 months). The judicial authorities' replies are used to update the AFCOS complaints table, from which the audit authority, the certifying authority and the Special Service for Institutional Support are informed of the progress of all complaints.
HU	Cooperation agreements have been concluded between the Directorate of Internal Audit and Integrity and the investigating authorities to **improve the flow of information.** A **tracking system** has been set up to follow up on investigations initiated following complaints.
IT	As already illustrated in Italian replies to previous questions, COLAF, in the framework of the guidance and orientation action constantly carried out in respect to all the Managing

	Authorities on the national territory, periodically provides specific directives which are elaborated on the basis of the innovations that have happened in the matter or of the criticalities detected over time on the basis of the experience gained in the field; most recently, last January, a specific circular was issued to all the competent Authorities with the subject "*Guidelines for improving the procedures for the compilation/implementation of the irregularity/fraud reporting forms in the IMS system" aimed precisely at overcoming certain criticalities detected at the central level, also following the continuous and profitable information exchange with the European Offices. M.S."* aimed precisely at overcoming certain critical issues detected at the central level, also as a result of the continuous and fruitful exchange of information with the European Offices. Specifically, in order to have a better guide and support the managing authorities in adopting correct, complete and consistent input and update procedures, the criticality profiles under examination and the relevant indications have been distinctly examined according to whether they are: a. **general aspects,** namely: (1) how to create, save and finalise the report case; (2) timing of case updates due to new developments; (3) cases relating to previous programming; (4) drafting of the Special Notice in cases of irrecoverability of sums to be brought to the charge of the European Union; (5) updating of cases already closed in IMS for which the relevant judicial/administrative/accounting proceedings are still ongoing; (6) timely monitoring of all cases in the system for which the Judicial Authority is known to be involved; b. **correct, complete and consistent implementation of the fields on the form,** with specific regard to the following aspects: (1) incorrect selection procedure when closing an IMS case; (2) incorrect allocation of codes in case of decertification of the EU amount and full recovery of the national share; (3) excessive use of generic codes in field 6.8 and correct and consistent implementation of field 6.9; (4) excessive use of generic codes in fields 7.2 and 7.3; (5) failing to indicate amounts for statutory interest in field 9.12; (6) omitted/incomplete/incorrect completion of Section 10; (7) incorrect representation of events in the "Comments" field - point 11.1 and omitted/incomplete/inconsistent entry of fields 11.3 and 11.4. As already pointed out on several occasions, among the issues subject to more in-depth analysis and more incisive awareness-raising with respect to the managing authorities to which the aforementioned note is addressed, there is undoubtedly that relating to the need to constantly and carefully monitor the judicial developments of the cases entered into the system, when the involvement of the Judicial Authority is known, including those closed for decertification or total recovery. On this matter, the possibility was reiterated that, in the event that a managing authority encounters difficulties in interacting with the judiciary, it may contact the Unit of the Guardia di Finanza for the repression of frauds against the European Union, as the Technical Secretariat of COLAF, which, also thanks to the specialised or territorial branches of the Guardia di Finanza, they will be able to seek proper solutions to facilitate the monitoring in question.
LV	If necessary, but not less than once a year, letters are sent to law enforcement authorities with a **request to provide information on the progress** of criminal

	proceedings. Since the EPPO started its operations , we have a certain procedure for communication, determined by the guidelines developed by the AFCOS's 'Criminal offences against the financial interests of the EU: definitions, typologies, signs and examples of practice'. Likewise, we hold informal consultations with investigators, prosecutors and communication through the AFCOS. We independently try to create an understanding through communication with employees from law enforcement institutions, explaining the details and nuances of our institution's needs and rationale, but systemic improvements have not been made so far.
PL	Regarding anti-fraud measures in the field of cohesion policy, the management and control system institutions have established cooperation links with external institutions. For example, the National Public Prosecutor and the minister responsible for regional development have concluded a cooperation agreement on providing information on ongoing and closed proceedings concerning projects co-financed by the EU. Under that agreement, there is a regular exchange of data on beneficiaries of EU funds who are under investigation. In addition, some institutions make use of the possibility put questions to the staff of the Public Prosecutor's Office when they need information promptly on ongoing proceedings. In accordance with existing sectoral procedures in the field of agriculture, when an institution refers a case to law enforcement authorities, it is obliged to keep the data on criminal proceedings in the relevant register of irregularities up-to-date until the proceedings come to an end. In the absence of information about the current stage of criminal proceedings, the competent institution must request up-to-date information from the law enforcement authorities conducting the investigation, and use it to update the data in the register. The verification of pending cases is carried out on a quarterly basis until the case is closed. Due to data confidentiality, it is sometimes difficult to obtain information from law enforcement authorities concerning ongoing cases, especially where the institution asking for information is not the entity that reported the case.
SK	Relevant authorities are obliged to **communicate with the competent authorities** and ask for updates on the current state of proceedings on a regular basis.

Digitalisation of the fight against fraud high on Member States' agenda

Q.2.1. Are you ensuring the digitisation of the fight against fraud is part of your NAFS?

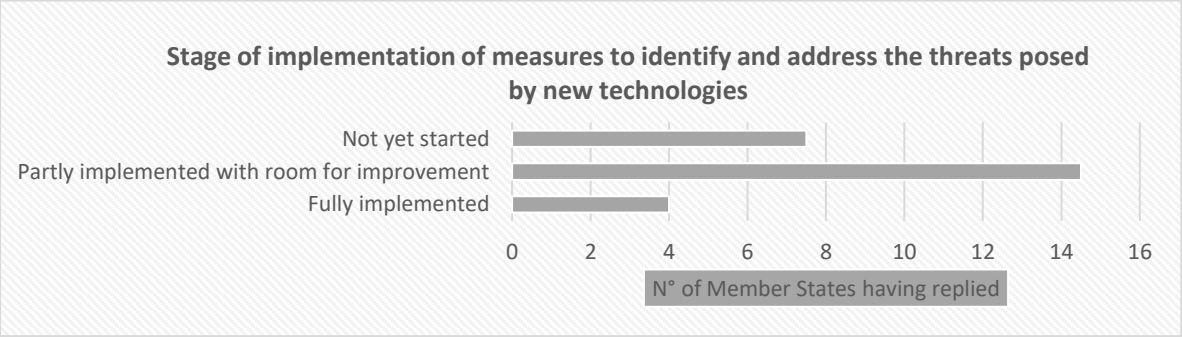
Most Member States (63%) have incorporated digitalisation of their fight against fraud into their NAFS. Since considering and implementing digitalisation is relevant to identifying existing and future threats arising from new technologies, it remains an area of concern. Several Member States have not yet integrated digitalisation as part of their NAFS. These Member States may need to be better prepared for the threat posed by digitalisation in the fights against fraud.

Digitalisation	Member State	Total
Yes	AT, BE, BG, DK, EE, EL, ES, FR, HU, IT, LV, LU, LT, MT, PT, SI, SK	17
No	CY, CZ, DE, FI, HR, NL, PL, RO, SE	9
n/a	IE[23]	1

Q.2.2 Have you implemented measures to identify and address the threats posed by new technologies?

While a few Member States (145%) have already fully implemented measures to identify and address the threats posed by new technologies, most Member States (54%) have only partly implemented some measures.

In other words, while most Member States have made a good start with the implementation of measures to identify and address the threats posed by new technologies, it is important that they continue investing in innovative measures to adequately address the future of technological developments in the fight against fraud.



[23] Ireland does not have an overarching national anti-fraud strategy. Relevant agencies and departments within the national system have operational expertise and engagement in EU fraud matters. Irish anti-fraud stakeholders include representatives from the shared management expenditure areas of the EU budget, Revenue Commissioners, individuals involved in reporting irregularities and others, such as the national police and security service (*An Garda Siochana*), auditors and public prosecutors. Each stakeholder is responsible for ensuring that efficient strategies and systems are in place to counter fraud and irregularities, and for ongoing monitoring and reporting.

Stage of implementation	Member State	Total
Fully implemented	DE, IT, PL, RO	4
Partly implemented some threat identification failures with room for improvement	AT, BE[24], BG, CZ, DK, EE, ES, FI, FR, HU, LV, LT, PT, SE, SI	14.5
Not yet started	BE[25], CY, EL, HR, MT, NL, LU, SK	7.5
n/a	IE	1

Q.2.3 If YES to Q.2.2. Can you explain and give some examples? If possible, please make a distinction between measures in relation to expenditure and measures in relation to revenue.

MS	Input
AT	Revenue-related: - **automate information exchanges** between authorities at national level - push to digitalise processes on financial management services for individuals and businesses; - **future use of artificial intelligence**, digitalisation and innovative technologies to identify certain patterns and for monitoring - more **data-based** anti-fraud measures; - gradual replacement of analogue procedures by electronic processes; - **use of predictive analytics** should already be taken into account when designing processes or IT procedures - extension of no-stop shops – i.e. application-free systems – or one-stop shops so necessary information needs to be provided only once. The human factor is still included in all processes.
BE	ERDF RBC Expenditure - new, improved database for the collection of data on ERDF - access to the UBO register of 'ultimate beneficial owners' for RRF for ***ex ante*** **and** ***ex post*** **verifications**
BG	An **analysis of the threats** posed by new technologies used in the management and control system of the EU funds and programmes is planned, along with recommendations and an action plan for addressing the identified risks and threats. The documents necessary for the implementation of a tender procedure are under preparation.
CY	n/a
CZ	REVENUE – electronic method of requesting tax information by law enforcement agencies; **identification of the legitimacy and legality** of requesting this type of information for criminal proceedings. EXPENDITURE – partial updates and new versions of monitoring systems IS MS 2014 and MS 2021; Under CAP: AMS – area monitoring system; increased protection for the external

[24] ERDF RBC, AGENSTSCHAP LANDBOUW EN ZEEVISSERIJ.
[25] ERDF Wallonia, AGENSTSCHAP LANDBOUW EN ZEEVISSERIJ.

	and internal perimeter of the information system of the State Agricultural Intervention Fund (SZIF); ARM – implementation of Active Risk Manager software (overview of fraud and irregularity risks); linking to state registers.
DE	General remarks: Germany, as a federal state, does not have a national anti-fraud strategy. In this context, however, we refer to p. 51 et seq. of Germany's Digital Strategy 2022-2025, (https://digitalstrategie-deutschland.de/static/fcf23bbf9736d543d02b79ccad34b729/Digitalstrategie_Aktualisierung_25.04.2023.pdf) Measures reported here have been taken at *Land* level. Replies from the *Länder* (ERDF) range from: 'Yes, fully implemented' via 'Yes, partly implemented' to 'No, not yet started'. Hanseatic City of Bremen: no NAFS, but Transparency Register used. Federal State of Lower Saxony: **risk description and risk assessment within the self-assessment tool,** including unauthorised access to IT equipment, IT systems and bank accounts, as well as hacking where it affects the intermediate body and the managing authority.
DK	Denmark does not have a NAFS covering all sectors. Denmark has **four sectoral national strategies for:** i) cohesion policy funds; ii) agricultural funds; iii) fisheries funds; iv) the Recovery and Resilience Facility. The Danish audit body has started implementing the anti-fraud IT tool, Arachne. It is expected that Arachne will be able to identify and address threats posed by new technologies. The audit body continuously monitors whether there are new risks, including risk from new technologies, that need to be addressed. If threats from new technologies arise, the audit body and the implementing bodies will design controls to mitigate the specific risks.
EE	An important technological innovation is **introduction of the surface monitoring system for agricultural area subsidies**, which is based on satellite monitoring technology, and can be used to detect and penalise falsified claims. Its use will be mandatory from 2023. An AI-based system to verify claims from geotagged photos will be developed later and also made mandatory. Other examples of the use of technology and data in anti-fraud activities in agriculture: • cross-use of data in ePRIA, the application acceptance service and application processing system of the Estonian Agricultural Registers and Information Board (PRIA), advancenotification system, and implementation of automatic checks; • risk management in the information system, automation of risk assessment; • integrating risk-based administrative control into the procedural system with the risk feedback system. The revenue area explains that there are general issues with data and data quality. Therefore, they have launched a **data management project** – describing all data based on the systems, so that it is in a standard format. They plan to create a **data warehouse.**

ES	On the revenue side, according to information from the State Tax Administration Agency, **specific controls have been designed for e-commerce**. Work is also underway with a view to using information on a massive scale to detect risk transactions. On the expenditure side, the utilities of the fund management software applications have been improved to allow more checks to be carried out through them (e.g. underlying procurement of contracting authorities and applications for the identification of SMEs in ApliFEMP, the monitoring software application used by FEMP, the Spanish Federation of Municipalities and Provinces). The Central Register of Beneficial Ownership has been created. Serving as a single central register for the whole of Spain, the register will collect and publish current beneficial ownership information relating to all Spanish legal persons, trusts, and similar unincorporated entities or structures operating in Spain. The information in the register will be accessible, free of charge and without restriction, to the authorities responsible for preventing, detecting, investigating and prosecuting terrorist financing, money laundering and predicate offences, both national and from other EU Member States. It will also be accessible to national authorities and bodies managing, verifying, paying or auditing European funds. In relation to the Recovery, Transformation and Resilience Plan, a 'data-mining' software tool (MINERVA) has been created at the State Tax Administration Agency. It is used by all managers of funds from the Recovery, Transformation and Resilience Plan to carry out a systematic analysis to prevent conflicts of interest in procurement and grant award procedures
FI	**The authorities responsible for the different EU-funded programmes are digitising their operations in line with their own assessments and resources.** For example, technical tools (infrastructure security tool, software code security tool, code dependency security tool, software vulnerability analysis tool) have been introduced and practical measures (security audit, including hacking and penetration testing conducted by external security experts) have been taken when implementing the Recovery and Resilience Facility (RRF).
FR	The Finance Act 2024, adopted on 29/12/2023, contains measures to combat fraud related to the use of new technologies. The Act: – granted a two-year extension of the experiment allowing tax and customs administrations to detect tax fraud through the collection and use of certain platform data online, and broadened the scope of the experiment; – allowed public finance officers to use pseudonyms to carry out active investigations on websites, social networks and messaging applications. These measures will help to combat revenue fraud and thus protect the EU's financial interests.
HU	**Security and protection measures** related to the monitoring and information system for managing EU funds (such as the implementation and operation of a

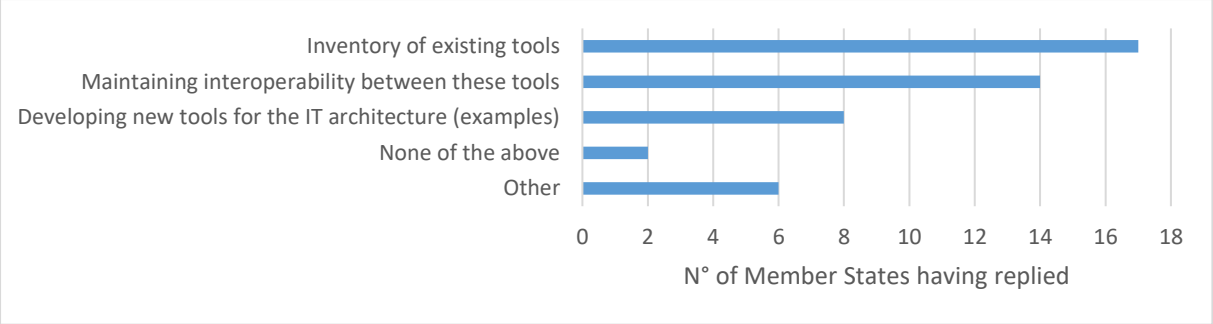
	two-factor authentication system).
IT	The Italian anti-fraud system comprises a comprehensive framework of agencies and police forces. All these bodies have internal structures dedicated to analysing crime and threats arising from new technologies. With specific reference to cybersecurity aspects, Decree-Law No 82 of 14 June 2021 established the Agency for National Cybersecurity (ACN) to protect security and resilience in cyberspace. In particular, the Agency has the following tasks: - prevent and mitigate cyberattacks, on national public and private entities that provide essential functions and services; - facilitate strategic technological autonomy in the digital sector; - evaluate IT products and services and carry out regulatory compliance inspections and audits in the field of cybersecurity; - deliver training to improve professional skills in the relevant professional sector and organise cybersecurity awareness and information campaigns.
PL	Poland has not adopted a national anti-fraud strategy (NAFS) and the European Commission does not oblige Member States to do so. There are direct possibilities for the digitalisation of the fight against fraud and the use of modern technologies in Poland by the relevant investigation services. The institutions involved in implementing EU funds are aware of the increase in the use of new technologies to commit criminal offences. They can engage indirectly in the digitalisation of the fight against fraud by using IT systems that support the processing of applications and grant agreements, and control of EU funds. In Poland, the CST2021 (*Centralny System Teleinformatyczny 2021*; 'Central IT System') applications are covered by **a development and maintenance agreement with a contractor for systems forming part of CST2021**. Maintenance services include, but are not limited to, administrator-level support ensuring correct functioning, high performance, security, availability and reliability of the systems and security of the systems and of the data stored and processed in them by the contractor. These services are intended to prevent any unauthorised access (including intrusion) and disruption or interruption of operation. Steps are continuously being taken to **identify possible gaps in digital skills, and a preventive approach** has been adopted. In the case of staff involved in the implementation and development of IT systems, employees have the opportunity to acquire new skills through various types of training, courses and study programmes in the field of information technologies. In addition**, technical support** is provided by the contractor under the development and maintenance agreement for those systems. For system users, manuals for the different applications are available in various forms (descriptive instructions, multimedia tutorials). **Continuous interactive training** is provided on how to use the systems, along with ongoing support from teams responsible for specific applications. Dedicated databases at the paying agency enable the recording of suspected and confirmed cases of fraud. These databases are used

	by all of the agency's organisational units (i.e. district offices, regional branches and the relevant departments at the head office) and entities carrying out delegated tasks that are involved in the detection of irregularities and fraud
PT	Revenue-related measures: – Development of a**n IT project linking up the reporting systems that are important for the logistics chain**. In this way, the risk analysis performed early in the logistics chain (pre-loading or pre-arrival) can be taken into account, in terms of the level of risk, the area of risk, the type of check and time for the check, so that the risk analysis takes place at the most appropriate time in the logistics chain, thus ensuring more effective and efficient risk mitigation. – Given the amendments to VAT legislation on the fight against VAT fraud in e-commerce in the EU (Central electronic system of payment information – CESOP), **draft legislation** was presented transposing Directive (EU) 2020/284 into Portuguese law. This resulted in the adoption of Law No 81/2023, which is still being implemented. – Through participation in EU-level **working groups,** we have been able to bring our practices into line with those of tax authorities in the other Member States, in particular on the definition of data structures and on the rules and communication mechanisms to be implemented in 2024. Expenditure-related measures: – Information security certification (ISO 27001) of the Institute for the Financing of Agriculture and Fisheries (*Instituto de Financiamento da Agricultura e Pescas* – IFAP, I.P.) – Certification of the Information Security Management System (*Sistema de Gestão de Segurança da Informação* – SGSI) maintained in accordance with ISO/IEC 27001:2013 (confirmed during the second follow-up audit). The SGSI has a systematic approach involving a series of policies, procedures, records, resources and related activities, which are managed collectively to protect the information assets. This approach is based on risk assessment and risk processing with a corresponding risk acceptance level. It is designed to manage risks effectively and implement the appropriate checks to ensure that the information assets are protected. – Development of application systems with densification at validation level. – **Awareness-raising and training activities** carried out by trainers and specialist IT (cybersecurity) bodies, and measures to raise awareness and **deepen knowledge of the use of tools** (e.g. Arachne) carried out by bodies using the management and control systems for EU funds.
RO	Implementation of the National Anti-Fraud Strategy (NAFS) has only just begun. The measures will be discussed in **working groups**, after which the decisions will be disseminated.
SE	This is a **work in progress** in terms of both analytical tools and tools for data collection, etc. For example, the Swedish ESF Council's 2024 action plan on anti-fraud measures includes **training initiatives** to combat organised financial crime. In this context, **AI is an area in which the authority is planning to develop skills.**
SI	Given the material competence of the Financial Administration, we **focus primarily on revenue-related measures**. For anti-fraud measures, we use the

	QlikView (QV) analytical platform and its updated successor QlikSense (QS). Within these platforms, we are developing new applications for specific aspects of customs (such as customs value, CP42 customs procedure, import, transit and export procedures, prohibitions and restrictions, including sanctions, excise duties, etc.) and taxes (type of tax, e.g. risk analysis in the field of corporate income tax). The purpose of the applications is to **identify the situation, trends, suspicious patterns, transactions and suspicious economic operators and, consequently, to carry out risk analysis and identify the most risky debtors.** The QlikSense platform also allows the use of machine learning, artificial intelligence, predictive analytics and questioning in natural language. This tool helps us take a more systematic approach to managing tax and customs risks by segment of taxable persons, key activities and risk groups, thereby helping the financial administration to achieve its objectives faster. In the fight against fraud, we also use the **KNIME software tool with the Rando Tree scientific model.** Based on reported data and the history of controls carried out, liable entities constitute the highest risk. We currently use the model for selecting controls in the field of corporate income tax. This method of selecting control entities complements traditional selection methods. Another software tool, **Fraud Management,** supports risk management using risk indicators (methods) that are key to identifying an individual risk. It allows for a quicker identification of risks on a large body of data and a simpler, centralised and more efficient allocation of cases to control bodies. The tool also requires control bodies to provide feedback to evaluate the suitability of the selected risk for control and, on this basis, the possibility of making 'pre-qualification analyses'. We also use **the SAP Business Objects Business Intelligence** suite, which enables data to be processed quickly and makes it possible to perform complex analysis of business data in real time, as well as to report and visualise it. The **Financial Administration** has identified the need to capture data from open source intelligence for controlling the growing trade through online shops and social networks (market place). For these purposes, we are planning to procure appropriate tools to obtain structured data at system level, which will be further analysed with the above-mentioned tools

Q.2.4 Does your strategy ensure one of these approaches to develop the IT architecture?

Most Member States have adopted a strategy that ensures various approaches to developing the IT architecture, in particular inventory of existing tools, maintenance of interoperability between these tools and the development of new tools for the IT architecture, see table below.



IT architecture	Member State	Total
Inventory of existing tools	AT, BE, BG, CY, CZ, DE, DK, EE, EL, ES, FI, IT, LV, MT, PL, RO, SI	17
Developing new tools for the IT architecture (examples)	AT, BE, CY, CZ, DE, ES, MT, SI	8
Maintaining interoperability between these tools	AT, DE, DK, CZ, EE, ES, FI, IE, IT, LV, LT, MT, PL, SI	14
None of the above	HR, LU	2
Other	CZ, FR, HU, IT, NL, SK	6

OTHER:

FR: One of the objectives of the French NAFS is to detect fraud by strengthening the collection of sharing and exploitation of data. Data collection involves, for example, the setting up by some administrations of an alert collection platform. As regards data sharing, managing authorities have started to consider setting up a single database to cross-check relevant information and avoid duplication financing. Data is analysed using European-level tools (such as Arachne or transaction network analysis (TNA)). National analytical tools have been developed to better target fraud (such as a tool for targeting flows customs). Also under discussion: the use of artificial intelligence in investigations to detect fraudulent entities as early as possible.

IT: On this point, Italy has established a comprehensive system that fully meets the need to prevent and combat fraud against the EU. Each institution, agency and body responsible for managing European resources in various capacities and according to its competences has over time set up a number of systems, applications, databases, methods and procedures to ensure effective prior assessment of the risk of fraud, corruption, conflict of interest and double funding in connection with EU budget implementation.

With regard to **budget revenue**, in particular **traditional own resources**,, in 2022 and 2023 **the Customs and Monopolies Agency** mainly used three methods to select and analyse customs declarations to detect fraud against the EU budget, particularly via under-invoicing.

- The first method is based on the value thresholds taken from the **Theseus** database operated by the Commission's Joint Research Centre. This is a statistical methodology to select declarations with a value below a fair price calculated at European level, hence at high risk of under-invoicing of imports, by identifying correct value ranges for goods.
- The second method, dubbed 'credibility', is another statistical approach which is used to select, at the time of customs clearance, import declarations that show statistical anomalies giving rise to a strong suspicion of under-invoicing of the declared import value.
- The third method uses a Python algorithm to detect all items having unit values (EUR/kg) considered to be abnormal, among declarations with an intrinsic value of less than EUR 150, hence benefiting from customs relief under Regulation (EC) No 1186/2009, and submitted by the main declarants,.

More generally, as part of its cooperation with EU bodies and with OLAF, the Customs and Monopolies Agency systematically analyses the entire information flow originating from those bodies, and on this basis prepares risk profiles and updates/amends existing profiles.

Similarly, as part of cooperation with the Commission and the other Member States' customs administrations, risk information forms from other Member States, competent EU bodies and Italian customs offices, are analysed with a view to entering or amending risk profiles.

In the area of investigations relevant to relations with the EPPO, a large number of analyses to detect fraud against the EU budget have been carried out, in particular:

- bimonthly review of national penal proceedings under the jurisdiction of the EPPO, to monitor the effectiveness of investigations into illegal conduct affecting the EU budget and to constantly assess the greater entitlements established by the Agency;
- use of the anti-fraud/AIDA database to examine the types of fraud recorded there so as to identify new criminal offences;
- analysis of imports from the UK by domestic operators, after Brexit, to verify correct use of the preferential origin of the goods and thus ensure that the goods would not be imported duty-free;
- analysis of alerts about administrative investigations conducted by OLAF and about possible evasion of customs duties, for the aspects under the specific jurisdiction of the European Public Prosecutor.

One of the databases most often used by the Customs and Monopolies Agency is **COGNOS**, which collects information on goods imported into the EU. For each product it provides the permitted value range within which the declared value of the goods may vary.

This database is fed with national and international data from customs declarations and recapitulative statements of intra-Community purchases and supplies. As a result, it possible to identify, with the greatest precision, for each tariff heading, the raw material used, the name of the importing company, the more or less well-known brands of the imported goods and hence the value and quality of products similar to the one being checked.

Other systems widely used for risk analysis in this sector include:

- **InDEx VIES**, to consult intra-EU transactions and then compare them with the tax data on the **SerPICo** application (acronym for *Servizio Per i Contribuenti*, a taxpayer service developed by the Revenue Agency and containing data from tax returns and other communications submitted by taxpayers);
- **ORBIS** which provides detailed information on corporate structures on a global scale; **OWNRES**, which collects cases of fraud relating to traditional own resources for amounts exceeding EUR 10 000; and
- **Theseus**, which provides the correct market price by type of goods, in order to identify under-invoicing offences.

As regards budget revenue, in particular **VAT**, the Italian Revenue Agency uses the computerised **TNA (transaction network analysis)** tool developed by the Commission within EUROFISC. TNA enables the acquisition and joint analysis of the information contained in the VIES system for all EU Member States. The tool is particularly useful in identifying parties involved in intra-EU VAT fraud schemes.

The intention for the coming years is to enhance risk analysis, for example through the use of new artificial intelligence and machine learning tools.

In terms of technological capabilities, a new anti-fraud analysis tool, **TAXNET**, has become fully operational. This tool makes a number of different databases (electronic invoices, master data, payments, VIES database, etc.) interoperable, so that it is possible to automatically reconstruct the entire fraud chain and rapidly map the links and recurrences between the various entities.

With regard to **budget expenditure**, risk assessment on **cohesion policy** funding is covered by the main control functions of the various **managing authorities.** These closely follow the Commission's '**EGESIF Guidance Note No 14-0021-00** of 16 June 2014 on **Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures**' and use the **Arachne** system extensively in accordance with the 'National Guidelines' drawn up by a dedicated national working group within the State General Accounting Department of the Ministry of the Economy and Finance.

At central level, **the Inspectorate General for Financial Relations with the European Union (IGRUE)**, also embedded in the State General Accounting Department is responsible for coordinating audit authorities and functions and has issued its own 'Manual of Audit Procedures' (Version 7 of 21 July 2021), which has a specific paragraph on risk assessment.

In this context, the IGRUE has developed a national risk assessment methodology, available on the MyAudit information system, which has a greater level of detail and some differences compared with the methodology in the EGESIF Guidance Note, especially regarding the risk score calculation.

The **Financial Police**, whose economic and financial police functions also encompass all types of infringements against the national and EU budgets, develops its risk analysis and assessment activities on both the **revenue** and **expenditure** sides.

To combat **VAT fraud, the Special Revenue Protection and Anti-Tax Fraud Unit (*Nucleo Speciale Tutela Entrate e Repressione Frodi Fiscali*)** performs permanent risk analysis to identify the companies suspected of involvement in fraud circuits, and delegates further investigations to the local units.

This analysis involves examining data from the **Eurofisc network**, which, since 2021, has been using the **TNA** system, an advanced analysis tool for identifying potential cases of EU VAT fraud rapidly and efficiently.

This information is cross-referenced with data from the many databases used by the Financial Police, including:

- **STAF** (*Strumento AntiFrode* - Anti-Fraud Tool), an application for effective monitoring of VAT-registered taxpayers to enabling those involved in tax fraud to be promptly identified and and risk score to be assigned to them;
- the **Fatture e Corrispettivi** (Invoices and Payments) portal and the **@-Fattura** (@-Invoice) application, which allow detailed and integrated analysis of electronic invoice data;
- **EMCS-eAD Dogane** (Customs) and **COGNOS - Dogane e Accise** (Customs and Excise), two applications that are used to monitor the movement of products subject to excise duty and of sector operators, and are especially useful for combating VAT fraud in the fuel sector;
- **COGNOS - area Analisi libera Italia** (Italy free analysis area), a partition of the '*Dichiarazioni doganali*' (customs declarations) area of the COGNOS business intelligence platform, which enables multidimensional processing using historical customs declaration data from the month preceding the query. This application is especially useful for selecting entities for post-clearance customs controls and conducting subsequent in-depth investigations where appropriate, and for any other investigative activities requiring the reconstruction of international trade flows, including from past periods.

Further specific analyses have been carried out by the Public Expenditure and Anti-Tax Fraud Unit to **combat undue offsetting and fraud in the transfer of** building and energy **tax credits**, including the 110% Superbonus scheme, a measure co-financed by the national RRP.

Some of the main applications used to this end are:

- **PRisMA - Portale Riscossioni Monitoraggi e Applicazioni** (Portal on Collections, Monitoring and Applications) – which allows precise consultation of taxpayers' subsidised tax credits and data on credit assignments;
- **Moni.C. - Monitoraggio delle Compensazioni** (monitoring of offsetting) – which allows both individual and massive searches, by processing the data from F24 tax payment forms, to detect undue offsetting of tax credits.

To improve effectiveness in preventing and detecting fraud against the EU budget, in 2022 the **Public Expenditure and Anti-EU Fraud Unit** handled the evolutionary maintenance of the **SIAF (Anti-Fraud Information System)**, an application implemented under a project

financed with resources from the national operational programme 'Governance and Technical Assistance 2007-2013'.

The SIAF is a business intelligence platform that supports operational analyses in the field of public expenditure.

By collating the elements acquired, including those from the other databases used by the Financial Police, it is possible to extract lists of public funding beneficiaries at risk of irregularities.

This resource, initially only available to the Financial Police Units located in the 'convergence objective' regions of the 2007/2013 Multiannual Financial Framework (Puglia, Campania, Calabria and Sicily), was extended to the whole of Italy in 2021.

With specific regard to the RRP, the **Public Expenditure and Anti-EU Fraud Unit of the Financial Police** - with the support of the unit at the Department for European Affairs of the Presidency of the Council of Ministers that acts as the technical secretariat of the Committee for combating fraud against the European Union - has prepared detailed **checklists** with specific risk indicators separately applicable to the disbursement of incentives or the execution of public works in the provision of services. Through the **ReGiS** system, developed by the State General Accounting Department, these checklists are made available to all central and local administrations and to the bodies implementing the RRP, enabling them to improve their independent capacity for identifying anomalous situations warranting further investigation.

An important recent addition to the Italy's toolbox of measures for strengthening risk analysis in EU fund management is the '**Integrated Anti-Fraud Platform (PIAF-IT**)', **created by the State General Accounting Department in collaboration with the Committee for combating fraud against the European Union** and co-financed by the European Commission (OLAF) with resources from the EU's 'Hercule III' programme. The platform fully responds to specific EU regulatory requirements and several Commission recommendations that emphasise the need to design and target audit and control activities on the basis of risk analysis and to develop IT tools capable of exploiting the enormous amount of data available to national and local authorities.

Q.2.5 For any approach selected, can you provide explanations of its implementation?

MS	Input
AT	**See 2.3**
BE	ERDF RBC and Wallonia ERDF and RRF: - **new, improved database** for the collection of data on ERDF - access (and for Wallonia Interoperability) to the **UBO register of ultimate beneficial owners for the RRF** (and the ERDF 21-27 for Wallonia) for *ex ante* and *ex post* verifications AGENSTSCHAP LANDBOUW EN ZEEVISSERIJ: We are looking to **rewrite existing tools** so we can easily access all the data to put it in to **fraud detection tools like Arachne.**

BG	The current strategy includes taking **inventory of existing tools**. Arachne and the Unified Information Systems (UMIS) are the basic instruments in the fight against frauds. UMIS contains complete financial and physical data at project level and almost all of it is structured data. Therefore, it allows all types of cross-checks and subsequent use and processing of the information. At the moment there are some operational interfaces between UMIS and several other systems and national databases such as Regix (enabling exchange of information between registries and introduced and supported by the Bulgarian E-Government Ministry), Monitorstat (National Statistical Institute Information System), and the National Registry Agency database. Interconnections with some other public registers and systems are also planned. These will further expand the scope for checks and analysis and reduce the risk of false information, fraud or unintentional mistakes and irregularities.
CZ	- Innovation of the main IT system, possibilities of sophisticated analyses – data mining. Implementation of an interconnection to public and non-public registers. - Certified systems such as CRIBIS, ARACHNE, Register of Beneficial Owners used to detect fraud, corruption and conflict of interest. - Annual assessment of the development of the State Agricultural Intervention Fund (SZIF)'s information system, an integral part of the SZIF's Information 'Concept'(i.e. it is a legal requirement).
CY	**1. Introduction of a new e-procurement system** Cyprus's General Accounting Office is implementing a contract for the **introduction of a new electronic procurement system and statistical reporting and analysis of public procurement data tool.** This is designed to: – provide a holistic solution based on emerging and modern technologies, supporting the once-only principle with benefits for all users, – support its interconnection with other services (e.g. Tax Department, Registrar of Companies, etc.), – allow for better management of framework agreements and dynamic market systems, – support the operation of an online shop for the management of products and the placing of electronic orders, – publish various statistics and information (both overall and at competition level), which the public and interested parties can process and analyse, enhancing transparency. The aim is for the system **to cover the whole lifecycle of a public contract, enabling users to have the information they need to draw useful conclusions on public procurement and identify recurrent patterns of awards/overruns of budget/changes and requirements, etc.** **2. Introducing professionalism in public procurement** On the basis of a decision of the Council of Ministers, the creation of the professional framework for public contracts to be implemented by the Cypriot General Accounting Office, which will cover the introduction of the role of professional buyer. The objectives of the project include **exploring international best practices** and adapting them to Cypriot data, creating a **scientific learning**

	plan for professional buyers and a plan to assess their ability to convert theoretical background knowledge into practical competence in their field of action. The project also contains measures relating to the use of tools provided for in the European Directives, such as competitive dialogue, dynamic purchasing systems, e-shopping, etc. Through the reform, it provides for: – the **establishment of a service centre** for contracting authorities where it is planned that a large proportion of public procurement procedures will be carried out by professionals trained in theory and on a practical level, drastically reducing the procedures to be carried out by staff from small contracting authorities who are insufficiently trained and trained. — The extension of the Framework Agreements, covering a larger range of services, supplies and works used horizontally, relieving contracting authorities of the administrative burden and reducing the legal risks arising, since the Framework Agreements will be taken over by Professional Buyers. **3. Creator of tender documents** The tool is in an implementation process and aims to standardise tender documents and help bidders prepare tender documents and select criteria in a way that avoids any attempts to change conditions that undermine competition.
DE	Hanseatic City of Bremen (ERDF): Use of the Transparency Register Lower Saxony (ERDF): Within the **self-assessment tool**, the operation of a web application firewall, a virus scanner at the intermediate body, the assigning of permissions according to user privileges, and the storing of an access matrix in the intermediate body's data centre. In addition, all IT systems are password-protected. IT security is described in the IT implementation concept within the management and control system and is continuously ensured by the service provider, *IT-Niedersachsen*. Access to all of the *Land* government's online services is protected by VPN.
DK	The Danish Business Authority report that they have numerous registers that they run checks on and compare in digital processes resulting in awareness lists used in manual checks. The Danish audit body report that they have **started the implementation of the anti-fraud IT tool Arachne.** When implemented it will be the primary IT tool used in the fight against fraud.
EE	In 2023 we **actively tested Arachne and** want to move forward with testing to determine whetherit may be used as a fraud risk detection IT tool in the future.
EL	**Special Service for Institutional Support and Information Systems: The technical infrastructure** has been implemented in the Integrated Information System in order to connect to the Central Register of Beneficial Owners.
ES	The general approach of the strategy is based on (1) carrying out a specific analysis of data sources and data analysis tools to enhance detection and developing guidelines to **facilitate the use of these data sources and tools,** (2) studying the **main mechanisms used in practice** to detect fraud in

	European funds to identify problems and best practices, as well as proposals for improvement, and implementing the conclusions reached, and (3**) improving fraud detection measures** by generalising the use of data analysis tools, and promoting other proactive detection methods. According to the information provided by the EMFF managing authority, the main objective of the Spanish e-Cohesion Network (RedeCo) is t**o coordinate the different participants** in Spain to meet the requirements of the applicable law on electronic relations between the different participants and authorities in order to optimise the design, implementation and normal operation of the different IT systems, thus favouring more agile, transparent and efficient operations in favour of the full effectiveness of cohesion policy. This main objective is complemented by a number of specific objectives: - to make an inventory of applications involved in 'e-cohesion' in Spain; - to share the concepts and solutions used in the construction of the information systems; and - to disseminate the roadmaps to ensure the coordinated implementation of the different milestones in the management of each of the Funds.
FI	For the RRF, **inventory of existing tools and dependencies and continuous technical analysis of existing tools.**
HU	In 2023, there were examples of **developing new tools and maintaining interoperability** between them, but these were outside the strategy for the development of the IT architecture. The examples include the introduction of the obligation to declare any conflict of interest in the 'EUPR' monitoring and information system, the extension of the anti-fraud function and certain developments related to the **submission of data to Arachne**. In response to the issues raised, Hungary has assessed the potential for improvement and taken action accordingly after appropriate planning and testing.
IE	For example, in relation to the Just Transition fund, the Enterprise Project Portfolio Management system allows for data to be extracted for upload to the Arachne system. At a future date this may be accomplished by an API (application programming interface).
IT	**Inventory of existing tools** The Italian AFCOS has long been active in this regard. Starting from the two-year period 2015-2016 it has designed and implemented projects for the preliminary benchmarking of the best administrative and police databases used by the central and local authorities to monitor and control EU funding, strengthen the fight against illegal practices and strengthen risk analysis, and provide Financial Police Units with guidance on controlling EU public expenditure ('National Anti-Fraud Database – DNA' project). Subsequently, the AFCOS devised the 'Integrated Anti-Fraud Platform (PIAF-IT)', a unique business intelligence tool that collects data from a variety of external sources at national and European level to

prevent and combat fraud and irregularities against the EU budget.

Maintaining interoperability between the tools

An important innovation in the digitalisation landscape to strengthen risk analysis in EU fund management is the aforementioned 'Integrated Anti-Fraud Platform (PIAF-IT)'.

PIAF-IT is an innovative business intelligence tool made available to the central and local public administrations engaged in controlling and/or implementing EU funds. The tool is used to collect and organise into specific reports (by means of a single - even 'massive' - query, and by applying multiple search parameters) all the key information that can be extracted from a specific dataset and that relates to the beneficiaries of European public funding and the RRF.

The data are collected from a variety of external national and European sources to consolidate and strengthen the fight against fraud and other illegal activities affecting the EU budget. PIAF-IT thus complements and supports the European IT system Arachne, and, in general, any other tool used in the fight against fraud, including at police force level.

The platform can be used to make online queries and generate a 'reputation factsheet'; it helps all national administrations managing EU funds to exchange information and, hence, optimise the sensitive but fundamental fraud prevention phase. Its aim is to centralise and display all key information on the beneficiaries of EU public funding and allow users to generate specific analysis outputs by querying a single computer system in an aggregated manner, without having to make several separate queries.

Continuous interoperability with the data sources integrated into PIAF-IT boosts the accuracy of the data exchanged and the continuous process of updating the information acquired. At present, the platform connects with the databases managed by the following entities:

- **Revenue Agency (Tax Register Information System)**, which plays a key role in conducting tax assessments and financial controls to combat tax evasion;
- **InfoCamere (Companies Register)**, to verify the actual legal existence of a company and its partners/shareholders, as well as its financial soundness;
- **Italian Court of Auditors** (**GIUDICO** - *Giustizia Contabile Digitale* - Digital Accounting Justice and **SIDIF** - *Sistema Informativo Irregolarità e Frodi* - Information System on Irregularities and Fraud), to obtain information on administrative court judgments in fiscal damage cases, thus providing a valuable tool for assessing a company's risk and likelihood of fraud;
- **Ministry of the Economy and Finance**, to verify whether the parties concerned received shared management funds, retrieve information on the checks carried out by the audit authorities on funded projects **(single data bank - BDU**), and check any fund payments for public works **(public administrations' database - *Banca Dati delle Amministrazioni Pubbliche* - BDAP**);

- **State General Accounting Department** (**Italian RRP monitoring and reporting system - ReGiS**), developed to support the management, monitoring, reporting and control of the RRP and ensure the electronic exchange of data between the various players involved in the governance of the national RRP;
- **Ministry of Enterprises and Made in Italy (National State Aid Register - RNA**), which can be consulted to find out whether beneficiaries have received previous State aid;
- **European Commission**, by interacting with European external sources, such as the **IMS**, which contains information on irregularities and fraud affecting the EU's financial interests, detected and reported by the Member States, and the **Financial Transparency System**, which provides information on the recipients of directly managed funds, so as to prevent and combat double funding;
- **Bureau van Dijk (ORBIS**), which contains comparable data on private companies worldwide.

The application, developed within an innovative technical framework that includes a technology based on microservices that can also store big data, offers a solution that is highly extensible in the future through actions to:

1. implement the platform's functionality by providing access to managing authorities and, with a supervisory role, to all public administrations in charge of controlling and monitoring funding, such as audit authorities and the Financial Police;
2. use additional data sources to acquire further subjective/objective data on the position to be examined and assessed, such as, for example,

- the '*Sistema Informativo del Casellario Giudiziale*' (criminal records information system) of the Ministry of Justice concerning convictions for specific fraud offences against the national and EU budget (PIF offences or other types of offences);
- the 'Kohesio' database managed by the European Commission's Directorate-General for Regional and Urban Policy (DG REGIO) for up-to-date data on projects and beneficiaries co-financed by the EU cohesion policy;
- the 'national public contracts database' of the National Anticorruption Authority to check the documentation proving that economic operators meet the general, technical-organisational and economic-financial requirements for participation in public tenders, supplies and services;
- the Antitrust Authority-AGCM's 'legality rating' tool, which provides an indicator of companies' compliance with high standards of legality).

Hence, the PIAF-IT anti-fraud IT platform is a model of interoperability at legal level (enabling actors operating in different legal environments to cooperate with each other), at organisational level (through the exchange of relevant information), at semantic level (as it ensures that the format and meaning of the exchanged data and information are preserved and understood during exchanges between parties), and at technical level (including specifications, data

	interconnection and integration services, and secure communication protocols).
LV	Existing data bases, information systems and **IT tools are constantly reviewed** to determine how to use them more effectively, which authorities need additional access to them, and which tools could be interconnected to perform checks automatically. For example, right now there is a project to interconnect the national e-procurement IT system with the IT system on taxpayers to automatically check if there are any conflicts of interest.
MT	The Maltese National Anti-Fraud and Corruption Strategy (NAFCS) requires that the systems already in place must be **examined and, where necessary, bolstered**. It also supports the procurement of additional software tools, where necessary, to enable a more professional approach with respect to analysis and investigations. A new application called **'Auditor's Toolkit'** was developed in 2023 by the Malta Information TechnologyAgency to enable the audit authority for EU funds to download documents related to any operation within the Structural Funds database at the click of a button. The system is currently at the testing stage. In line with action points 13 and 14 of the NAFCS and with Malta's RRP commitments, a central documentary repository system will be designed and created by Q4/2024 to **strengthen collaboration between national authorities** forming part of the coordinating committee, set up under the Internal Audit and Financial Investigations Act (Cap. 461 of the Laws of Malta). The system will (i) store electronic documents, (ii) offer centralised access to documents that can be easily retrieved by national institutions forming part of the coordinating committee, and (iii) provide the necessary security for sensitive information. In addition, the managing authorities for EU funds maintain interoperability between the Structural Funds database, the RRF database, the funding entities database, national databases (natural persons) and the CION Arachne database. Additional features will be included in the new programming period's management control system.
NL	Please see the questionnaire on the 2023 PIF report submitted by the Netherlands. The development of the NAFS is still in progress in the Netherlands. As the NAFS is currently not implemented, this does not cover the digitalisation of the fight against fraud or other aspects of the anti-fraud strategy. Therefore the questions in this section are answered 'no' as they are not applicable.
PT	Promoting the linking up of the reporting systems that are important for the logistics chain. In this way, the risk analysis performed early in the logistics chain (pre-loading or pre-arrival) can be taken into account, in terms of the level of risk, area of risk, type of check and time for the check, so that the risk analysis takes place at the most appropriate time in the logistics chain, thus ensuring more effective and efficient risk mitigation. On the expenditure side, as regards the management of EU funds, steps have been taken **to link up the various national authorities responsible**, with a view to ensuring the interoperability of the information systems to avoid double

	funding.
RO	Implementation of the National Anti-Fraud Strategy has only just begun The topics will be discussed in **working groups**, after which the decisions will be disseminated.
SI	Ministry of Cohesion and Regional Development: In our sectoral anti-fraud strategy, we have a set of existing IT support mechanisms in Slovenia, which helps to verify and prevent fraud, including some nationally-funded applications that are suitable for data mining and the managing authority's information system through which cohesion policy is implemented (declarations, checks, controls, disbursement of funds). The managing authority's IT system is closely linked to the national accounting system. This facilitates checks on similar entries in the system. Reply from the financial administration to question 2.5: Inventory of existing tools: - QlikView (QV) analytical platform and its updated successor QlikSense (QS); - ENIME software tool with Random Tree scientific model; - fraud management (FM); - SAP Business Objects Business Intelligence suite. Within the existing tools, **the financial administration is developing new applications for customs risk analysis and management. All existing applications are developed in such a way that they are interoperable.** Their use will also provide an audit trail and data protection, thereby ensuring data security requirements are met.
SK	The Slovak NAFS **emphasises the need to use all available IT tools (including Arachne)** in the fight against fraud and calls on the relevant authorities to employ these tools in their activities to the prevention and detection of cases of fraud and other irregularities. Nowadays, the relevant authorities implementing EU funds in Slovakia actively use Arachne to identify projects which present high risk of fraud, conflict of interest and other irregularities.

Q.2.6 Have you taken steps to identify and address skills gaps in digitisation?

A little over half of the Member States (56%) have indicated that they have taken steps to identify and address skills gaps in digitalisation.

Steps taken	**Member State**	**TOTAL**
Yes	AT, BG, CZ, DE, DK, ES, FI, IE, IT, MT, PL, PT, SE, SI, SK	15
No	BE, CY, EE, EL, FR, HR, HU, LT, LU, LV, NL, RO	12

Q.2.7 If YES to Q.2.6. What are the main gaps you have identified? How do you intend to address them?

MS	Input
AT	Deficit: **lack of know-how among users** Measures: necessary **upskilling and training** in the field of digitalisation.

BE	n/a
BG	An analysis of the skills gaps in digitalisation is planned as part of a more comprehensive **analysis of the skills and competence** of the staff working with EU funds and programmes. The aim is to develop an effective and tailor-made **training programme** for 2021-2027 and deliver relevant training on a regular basis or on demand.
CY	n/a
CZ	**Lack of knowledge** of the human resources involved - **training**, integration of resources into work activities. **Regular audit** is conducted by an external body within the Information Security Management System (ISO 27001:2013). Recommendations from audit findings are subsequently addressed. The information concept of the State Agricultural Intervention Fund is reviewed on a regular annual basis.
DE	Federal State of Lower Saxony (ERDF): **Continuous development** of digitalisation and IT systems. Required under banking supervision law.
DK	The Danish Business Authority report that they have not identified any at this point. If or when a gap is identified and the expertise is not available in house, **external expertise** will be hired.
ES	While efforts are being made to improve the use of data for both prevention and detection, as well as coordination, some of the problems that have been identified are: - **limitations in access** to some databases, for example from the Tax Agency or the Social Security; - regularity and ease of exchange of data and information, due to privacy and data protection issues; - lack of analysis and tools to analyse data as part of financial investigations; - limited access to information for investigation and asset tracing; - limited interoperability or lack of interoperability between public databases; - need for improved coordination between different entities. All approaches to address the identified gaps include improved access to databases through different **legal instruments,** improvements in the use of data and analysis tools that can identify red flags and help detect cases of fraud, as well as interoperability of databases, including data quality.
FI	For example, by taking into account developments in data science, including **artificial intelligence.**
IE	For example, an anti-fraud policy has been developed for the Eastern and Midland Regional Assembly which specifically deals with the EU Just Transition Fund. Arachne training has been received and anti-fraud training for delivery partners will follow.
IT	All central administrations and police forces play a key role in strengthening the digital architecture by disseminating shared tools and strategies for interconnecting national and European databases. In addition to establishing objectives, procedures and priorities for implementing

	the digital transformation, the main gaps in basic digital skills have also been identified. These include, in particular, the need for more resources specialising in the technical management and use of digital media and services. To meet this need, providing ad hoc training is one of the initiatives included in the National Strategy (NAFS). The goal is to pursue key objectives and measures in a joint and coordinated manner, with a view to accelerating the spread of digital culture in Italy so as to prevent and combat irregularities and fraud affecting the EU's financial interests. In this regard, among the projects developed in partnership with Italian and other EU Member States' universities, two initiatives should be mentioned, as they address the anti-fraud coordination tasks of the Italian AFCOS. - Participation in the still ongoing project '**Fraud Repression through Education (FRED 2**)', developed via institutional collaboration with 'La Sapienza' University of Rome and based the cooperation between several Italian universities, European universities (Belgium-Leuven, Finland-Rovaniemi, Greece-Athens) and the AFCOS of the respective participating countries. The initiative is being developed through a number of meetings and workshops aimed at setting up a European task force composed of academics and professionals that will produce a pilot study for the analysis of risk profiles for illegal behaviour or the improper use of EU funds, also linked to the use of new technologies. In parallel, a standing observatory is being set up to collect knowledge and experience in the development of innovative information systems to improve the prevention of and responses to irregularities and fraud against the EU. This includes greater use of digitalisation and technology to increase the efficiency and quality of controls and audits. - Participation in an ad hoc working group, composed of national experts and representatives from OLAF, AFCOS and other Commission departments, and tasked, under the aegis of the 'Advisory Committee for Fraud Prevention Coordination' (COCOLAF), with drawing up a compendium of the IT tools for managing and controlling planned reforms and investments, mainly those planned under the RRF.
MT	The managing authorities of EU funds identified **awareness** as a gap. An external information security specialist delivered **training sessions** for internal staff to address this issue. Further training is planned to ensure that the members of the coordinating committee have the necessary skills to make proper use of the central documentary repository system.
NL	n/a – Please see the questionnaire on the 2023 PIF report submitted by the Netherlands. The development of the NAFS is still in progress in the Netherlands. As the NAFS is currently not implemented, this does not cover the digitalisation of the fight against fraud or other aspects of the anti-fraud strategy. Therefore the questions in this section are answered 'no' as they are not applicable.
PL	Register of existing tools – all CST2021 systems are subject to registration and review as regards their changing usefulness and the current needs of the users;

	all substantiated business needs are addressed as part of the IT tool development services provided by the contractor. With respect to maintaining interoperability between these tools, full 'cooperation' as regards computerisation is maintained and developed between the CST2021 systems. At present, the different systems are fully interoperable, making it possible for the data collected in one system to be used in another system (where necessary and in line with the developments in this regard). In addition, in one of the systems where the primary objective is to present data from both internal databases and external public registers, work on adding further data sources is ongoing (the system has been built in such a way that it is relatively simple to connect new databases to it and to link data from those databases to the data that are already in the system). The conceptualisation of the **development of existing IT tools** – digitalisation in the area of implementation, management and control of cohesion policy programmes and the National Recovery Programme (including in the area of anti-fraud measures) is currently at a relatively advanced stage in Poland. For this reason, current activities in the area of digitalisation focus mainly on **further development of existing IT tools**, including the introduction of new, and improvement of existing, functions.
PT	The Ministry of Agriculture's digital transformation programme is made up of **six initiatives or projects,** including structural project No 5 Fraud and Inspection, which provides for a fraud control system and an inspection system.
SI	Ministry of Cohesion and Regional Development (MKRR) We have made a commitment to properly linking the national IS OU database used for the implementation of cohesion policy with the Arachne application, which will serve as a **data-mining tool** for all levels in the country (and beyond) and when reviewing links (related companies, related persons, etc.) Financial Administration (FURS) With regard to digitalisation, we estimate that the gaps in the protection of the EU's financial interests are minimal. We close the gaps by using **predictive analytics,** targeted selections of economic operators, equal treatment of all economic operators and the application of all other deterrent measures.

Reinforcing anti-fraud governance in the Member States

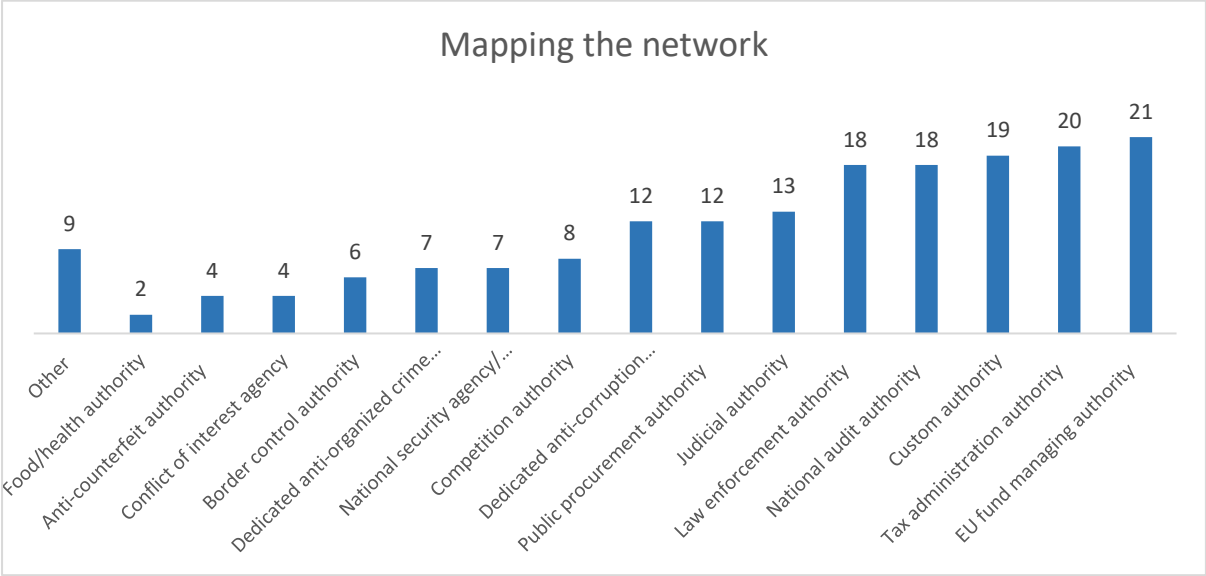
Q.3.1 Do you have an anti-fraud cooperation network in place?

The survey shows that most Member States have an anti-fraud cooperation network in place (81.5%) or one in development (15%).

Anti-fraud cooperation network	**Member States**	**Total**
Yes	AT, BG, CY, CZ, DE, DK, EE, EL, ES, DI, FR, HR, HU, IT, LV, MT, PL, PT, RO, SE, SI, SK	22
Yes, in development	BE, NL, IE[26], LT	4
No	LU	1

Q.3.2 If YES to Q.3.1, which authorities are part of this network?

Most Member States work together with various authorities. The following agencies are best represented in the national networks of anti-fraud cooperation: EU fund managing authorities, tax administration authorities, customs authorities, national audit authorities, and law enforcement authorities. The table below shows the various agencies that are represented (and how often) within the network.



Authorities involved	**Member States**	**Total**
Custom authority	AT, BE, BG, CY, CZ, DK, EE, EL, ES, FR, HR, HU, IT, LV, LT, NL, RO, SI, SK	19

[26] A network for anti-fraud cooperation with cross sector involvement was established in 2014 but engagement was limited in recent years by the consequences of a changed work environment during the COVID-19 pandemic. It is intended to re-engage and develop this network further.

EU fund managing authority	BE, BG, CY, CZ, DE, DK, EE, EL, ES, FR, HR, HU, IT, LV, LT, PL, PT, RO, SE, SI, SK	21
Law enforcement authority	BG, CY, CZ, DE, DK, EE, ES, FR, HR, HU, IT, LV, LT, PL, RO, SE, SI, SK	18
Tax administration authority	AT, BE, BG, CY, CZ, DK, EE, EL, ES, FR, HR, HU, IT, LV, LT, NL, PL, RO, SI, SK	20
Judicial authority	BG, CY, CZ, DK, EE, FR, HR, HU, IT, PL, RO, SI, SK	13
National audit authority	BE, BG, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LV, PL, PT, RO, SE, SI, SK	18
Anti-counterfeit authority	BG, FR, HR, IT	4
Food/health authority	BG, IT	2
Public procurement authority	BG, CY, EE, EL, ES, HR, IT, LV, NL, RO, SE, SK	12
Border control authority	BG, EE, ES, FR, HR, IT	6
Competition authority	BG, EE, FR, IT, LV, RO, SE, SK	8
Dedicated anti-corruption agency	BG, DE, EE, ES, FR, IT, LV, LT,PL, PT, RO, SI	12
Dedicated anti-organised crime agency	BG, FR, IT, LT, PL, RO, SE	7
Conflict of interest agency	BG, HU, IT, RO	4
National security agency / intelligence body	AT, BG, EE, FR, PL, SE, SK	7
Other, (please specify)	BG, EE, EL, ES, HR, IT, MT, RO, SK	9

Q.3.3 To what extent are (national) law enforcement and judicial authorities collaborating with the national anti-fraud network?

Most Member States (59%) indicate that their national law enforcement and judicial authorities are actively involved and collaborate within their national anti-fraud network. Several remaining Member States (26%) report that the collaboration is moderate, with room for improvement.

Degree of involvement	**Member State**	**Total**
Actively involved	BG, CY, CZ, DE, ES, FI, FR, HR, HU, IT, MT, PL, RO, SE, SI, SK	16
Moderately involved with room for improvement	BE, DK, EE, EL, LV, NL, PT	7
In the early stages of involvement	LT	1
Not involved at the moment	-	

Not applicable	AT, IE, LU	3

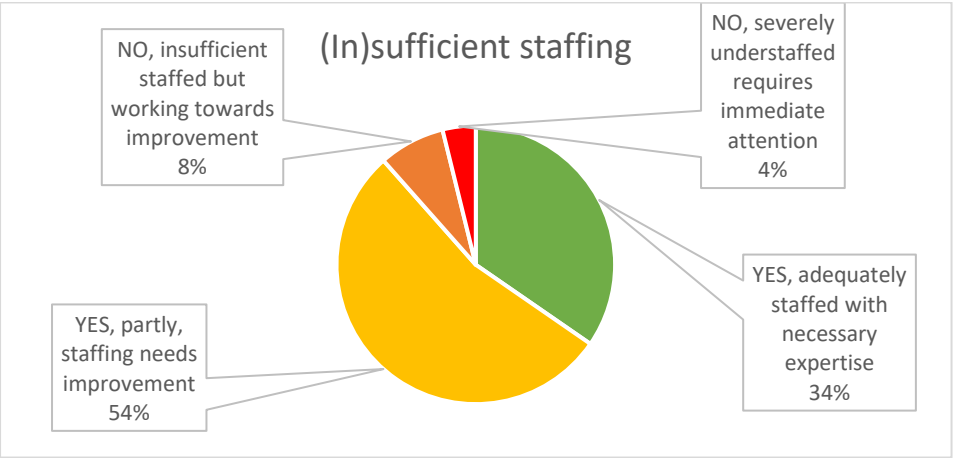
Q.3.4 Is your national anti-fraud network actively including cooperation with one of the following EU judicial and law enforcement authorities?

Almost all Member States actively cooperate with EU-level authorities, in particular with OLAF and EPPO, as can be seen in the overview below.

In collaboration with EU judicial and law enforcement authorities	**Member State**	**total**
Eurojust	CY,CZ, DE, HR, MT, RO	6
Europol, via national liaison office	AT, CY, CZ, DE, ES, FI, HR, IT, LT,MT, NL	11
EPPO, European delegated persecutor	AT, BE, CY, CZ, DE, EE, EL, ES, FI, FR, HR, IT, LV, MT, NL, PT, RO, SI, SK	19
OLAF	AT, BE, BG, CY, CZ, DE, DK, EE, ES, FI, FR, HR, HU, IT, LV, LT, MT, NL, PL, PT, RO, SI, SK	23
None of the above	LU, SE	2

Q.3.5 Are the national structures coordinating the anti-fraud network properly staffed to effectively manage and oversee anti-fraud activities?

Most Member States (85%) have sufficient staff to manage and oversee anti-fraud activities within their national structures. However, among the majority of the Member States that indicate that they have enough staff, over half point out that there is a need to improve staff expertise.



Staff	**Member State**	**Total**
YES, adequately staffed with necessary expertise	AT, BG, CZ, DE, DK, EL, HU, IT, SI	9
YES, partly, staffing needs improvement	CY, EE, ES, FI, FR, LU, LV, MT, NL, PL, PT, RO, SE, SK	14
NO, insufficient staffed	BE, LT	2

but working towards improvement		
NO, severely understaffed requires immediate attention	HR	1

Q.3.6 How do you ensure adequate staffing in your national structure?

In general, the various methods listed below are considered effective, ensuring adequate staffing at the national level, particularly those bringing staff from various executive and investigative body together, implementing cooperation.

Methods	**Member State**	**Total**
Capacity-building training	BG, CY, CZ, DE, EE, EL, ES, IT, PL, PT, RO, SI, SK	13
Giving new guidance on applying procedures properly	BE, BG, CY, CZ, DE, EE, EL, ES, HU, IT, PL, PT, RO	13
Bringing staff from various executive and investigative body together, implementing cooperation	BE, BG, CY, CZ, DE, DK, EE, EL, ES, FR, IT, LT, LU, LV,NL, PL, RO, SI, SK	19
Other (specify)	AT, BE, FI, HR, MT, RO	6