EUROPEAN
COMMISSION

Brussels, 3.9.2020
SWD(2020) 158 final

COMMISSION STAFF WORKING DOCUMENT

Follow-up on recommendations to the 30th annual report on the protection of the Union's financial interests and the fight against fraud - 2018

Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

31st Annual Report on the protection of the European Union's financial interests - Fight against fraud - 2019

{COM(2020) 363 final} - {SWD(2020) 156 final} - {SWD(2020) 157 final} -
{SWD(2020) 159 final} - {SWD(2020) 160 final}

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AEO: Authorised Economic Operator
AFCOS: Anti-Fraud Coordination Service
CAPs: Customs Automated Processing System
CIS: Customs Information System
EC: European Commission
ECA: European Court of Auditors
ENS: Entry summary declaration
ERDF: European Regional Development Fund
ESF: European Social Fund
EPPO: European Public Prosecutor's Office
IMS: Irregularity Management System
LVCR: Low-value consignments reliefs
MA: Managing Authorities
NAFS: National Anti-Fraud Strategies
PIF: Protection of the EU's financial interests
TFEU: Treaty on the Functioning of the European Union
TOR: Traditional Own Resources
UCC: Union Customs Code
UCC DA: Union Customs Code delegated act
UCC IA: Union Customs Code implementing act
UPU: Universal Postal Union
VAT: Value added tax

EXECUTIVE SUMMARY

In the 2018 Article 325 TFEU Report on the protection of the European Union's financial interests ('PIF report'), the Commission made two recommendations to the Member States, one for the revenue side and one for the expenditure side of the budget. This staff working document collects and summarises the Member States' replies for follow-up on the 2018 PIF report's recommendations, and provides updated information, initiatives and measures taken in 2018 and 2019 in the respective areas of revenue and expenditure.

A. REVENUE (Recommendation 1)

Member States are asked to enhance and enforce their customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR) and to ensure proper TOR collection.
Therefore, Member States are requested to ensure that:

- **electronic customs declaration systems do not automatically apply claimed duty relief on goods with the declared intrinsic value above EUR 150, on commercial consignments declared as gifts and on goods ineligible for relief;**
- **electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly;**
- **specific control measures are in place to prevent artificial splitting of consignments, aiming to benefit from duty relief; and**
- **ex post controls include verifications on traders' compliance with customs duty relief for low-value consignments and that authorised economic operators (AEOs) are not excluded from such compliance checks.**

As concerns customs control strategies for cross-border e-commerce trade, and in particular the potential abuse of low-value consignments reliefs (LVCR), 12[1] Member States have implemented this in full, 12[2] reported partial implementation, and 3[3] have not implemented it. The measures taken range from focused risk profiles for undervaluation, which cover low-value consignments, to upgrades and improvements of the Member States' customs systems.

Several Member States have taken specific measures to deal with this recommendation. For example, Greece's operational plan for the independent authority for public revenue (IAPR) includes quantitative targets for controls on e-commerce consignments. Luxembourg Customs deployed an IT solution dedicated to electronic risk analysis of structured pre-arrival consignment-level data related to low-value consignments. Hungary drew up a strategy dedicated to cross-border e-commerce taking into account the recommendation of the 2018 PIF report. Romania focused on the improvement of cooperation between public authorities, national and international organisations in the field of fraud in cross-border e-commerce. Finland has a control plan, 'Undervaluation through e-commerce'.

[1] Germany, Estonia, Ireland, Spain, France, Latvia, Luxembourg, Hungary, the Netherlands, Austria, Slovenia and Slovakia.

[2] Belgium, Bulgaria, Czechia, Greece, Italy, Lithuania Poland, Portugal, Romania, Finland and Sweden.

[3] Croatia, Cyprus and Malta

In addition, the Member States were requested to ensure that:

a) Electronic customs declaration systems do not automatically apply claimed duty relief on goods with the declared intrinsic value above EUR 150, on commercial consignments declared as gifts and on goods ineligible for relief. The follow-up for 2018 showed that 15 Member States[4] replied that they are fully implementing this recommendation and 9[5] reported partial implementation. Three Member States[6] have not implemented it.

b) Electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared foods under LVCR by means of risk profiles or randomly. In the follow-up for 2018, 16 Member States[7] replied that they fully implemented this recommendation and 11[8] reported partial implementation.

c) Specific control measures are in place to prevent artificial splitting of consignments, aiming to benefit from duty relief. In the follow-up for 2018, 9 Member States[9] replied that they are fully implementing this recommendation and 13[10] reported partial implementation. Five Member States[11] have not implemented it.

d) Ex post controls include verifications on traders' compliance with customs duty relief for low-value consignments. In the follow-up for 2018, 14 Member States[12] replied that they fully implemented this recommendation and 11[13] reported partial implementation. Two Member States[14] have not implemented it.

e) Authorised economic operators (AEOs) are not excluded from such compliance checks. Most Member States[15] have implemented this recommendation in full; two[16] have not implemented it.

B. EXPENDITURE (Recommendation 2)

[4] Belgium, Czechia, Estonia, Ireland, France, Spain, Latvia, Luxembourg, Cyprus, Hungary, Austria, Portugal, Romania, Slovenia and Slovakia

[5] Bulgaria, Denmark, Germany, Greece, Croatia, Italy, Lithuania, Poland and Sweden

[6] Malta, the Netherlands and Finland

[7] Denmark, Germany, Spain, France, Italy, Latvia, Luxembourg, Hungary, Malta, Lithuania, the Netherlands, Austria, Poland, Portugal, Slovenia and Slovakia.

[8] Belgium, Bulgaria, Czechia, Estonia, Ireland, Greece, Croatia, Cyprus, Romania, Finland and Sweden

[9] Germany, Estonia, Greece, Latvia, Luxembourg, the Netherlands, Austria, Slovakia and Sweden.

[10] Bulgaria, Ireland, Spain, Croatia, Italy, Cyprus, Hungary, Lithuania, Poland, Portugal, Romania, Slovenia and Finland.

[11] Belgium, Czechia, Denmark, France and Malta.

[12] Germany, Ireland, Spain, France, Italy, Cyprus, Latvia, Luxembourg, Lithuania, Malta, Austria. Romania, Slovenia and Slovakia.

[13] Belgium, Bulgaria, Czechia, Estonia, Greece, Hungary, the Netherlands, Poland, Portugal, Finland and Sweden.

[14] Denmark and Croatia.

[15] Bulgaria, Czechia , Germany, Denmark, Estonia, Ireland, Greece, Spain, France, Croatia, Lithuania, Italy, Cyprus, Latvia, Luxembourg, Hungary, Malta, the Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Finland and Sweden.

[16] Belgium and Slovakia.

The Commission reiterates the appropriateness of Member States that have not already done so to adopt national anti-fraud strategies.
These strategies should be developed in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services.
In line with what was recommended in previous years, these strategies should take into account:

- **the risk analysis conclusions contained in this and previous reports;**
- **the need to structure the coordination between administrative and criminal checks and investigations;**
- **how to incorporate tips from media and whistleblowers in the control system; and**
- **the opportunity to strengthen the risk analysis based approach to detect irregularities and fraud, including the use of IT tools (such as ARACHNE).**

As concerns the recommendation to the Member States which have not already done so that they adopt national anti-fraud strategies, (NAFS), these should be developed in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU's financial interests, including law enforcement and prosecution services. In line with what was recommended in previous years, these strategies should take into account a) the risk analysis conclusions contained in this and previous reports and b) the need to structure the coordination between administrative and criminal checks and investigations.

The follow-up for 2018 showed that 10 Member States reported that they have adopted or updated a NAFS which they have communicated to the Commission (OLAF)[17], whereas 17 have not adopted a NAFS.[18] Four Member States are considering adopting or are in the preparation stage of a new NAFS, not yet communicated to the Commission (OLAF).[19]

Nine Member States have fully developed their NAFS in cooperation with all bodies and authorities that have expertise in the area of the protection of the EU's financial interests, including law enforcement and prosecution services[20]. Three MS have partly implemented this[21] and 1 has not implemented it[22]. This recommendation was not applicable to the remaining 14 Member States as they have not done any work on a NAFS yet[23].

Seven Member States developed their NAFS fully taking into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports.[24] Five Member States

[17] Bulgaria, Czechia, Greece, France, Italy, Latvia, Hungary, Malta, Austria and Slovakia
[18] Belgium, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Luxembourg, Lithuania, Netherlands, Poland, Portugal, Romania, Slovenia, Finland, Sweden.
[19] Belgium, Spain, the Netherlands, Romania.
[20] Bulgaria, Czechia, Greece, Italy, Latvia, Hungary, Malta, Romania and Slovakia
[21] France, the Netherlands, Sweden
[22] Austria
[23] Belgium, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Lithuania, Luxembourg, Poland, Portugal, Slovenia, Finland.
[24] Bulgaria, Greece, Italy, Latvia, Hungary, Malta, Austria and Romania

implemented this partially[25] whereas 2 Member States have not implemented it[26]. This recommendation was not applicable to the 13 remaining Member States[27].

Eight Member States have developed a NAFS that fully takes into account the need to structure the coordination between administrative and criminal checks and investigations[28], 5 have implemented this part of the recommendation partially[29] and 1 did not implement it.[30] This recommendation was not applicable to the 13 remaining Member States[31]. Five Member States made an assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests[32]; 9 have not done so[33]. This recommendation was not applicable to the 13 remaining Member States[34].

The Member States were recommended to strengthen their risk analysis to detect irregularities and fraud, including the use of IT tools (such as ARACHNE), to share results deriving from the use of findings in the PIF reports in their fraud risk assessments and to further exploit the potential of risk analysis, tailoring the approach to the different types of expenditure. On the detection of irregularities and fraud including the use of IT tools (such as ARACHNE), 16 Member States have fully implemented it[35], 10 have partly implemented it[36] and 1 has not provided information[37]. Thirteen Member States made use of ARACHNE during their risk analysis[38]. The majority of Member States uses a combination of national and other publicly available tools.

As concerns the sharing of results deriving from the use of the PIF Report's findings in their fraud risk assessments, 16 Member States shared their results[39] and 9 did not have any results to report[40]. One Member State has not provided information.[41]

---

[25] Czechia, the Netherlands, Portugal, Slovakia and Sweden

[26] Austria and Malta

[27] Belgium, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Lithuania, Luxembourg, Poland, Sweden and Finland.

[28] Bulgaria, Greece, Italy, Latvia, Hungary, Malta, Austria and Romania

[29] Czechia, the Netherlands, Portugal, Slovakia and Sweden.

[30] France

[31] Belgium, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Lithuania, Luxembourg, Poland, Slovenia and Finland.

[32] France, Italy, Latvia, Austria and Romania

[33] Bulgaria, Czechia, Greece, Hungary, Malta, the Netherlands, Portugal, Slovakia and Sweden

[34] Belgium, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Lithuania, Luxembourg, Poland, Slovenia and Finland.

[35] Bulgaria, Czechia, Germany, Greece, Croatia, Italy, Latvia, Luxembourg, Hungary, Malta, the Netherlands, Austria, Poland, Portugal, Romania and Slovakia.

[36] Belgium, Denmark, Estonia, Ireland, Spain, France, Cyprus, Slovenia, Finland and Sweden.

[37] Lithuania.

[38] Belgium, Bulgaria, Czechia, Denmark, Ireland, Italy, Latvia, Hungary, Netherlands, Portugal, Romania, Slovenia and Slovakia.

[39] Belgium, Bulgaria, Czechia, Germany, Estonia, Greece, Croatia, Italy, Cyprus, Latvia, Luxembourg, Hungary, Poland, Portugal, Slovenia and Slovakia.

[40] Denmark, Ireland, Luxembourg, Malta, the Netherlands, Austria, Romania, Finland and Sweden.

Regarding the exploitation of the potential of risk analysis, tailoring the approach to different types of expenditure, follow-up on the recommendations for 2018 showed that 15 Member States have fully implemented this recommendation[42], 11 have partly implemented it[43] and 1 has not implemented it[44]. One Member State has not provided information[45].

As regards cross-cutting issues, the Commission recommended that the Member States facilitate and assess the spontaneous reporting of irregularities and strengthen the protection of whistleblowers. Thirteen Member States have implemented this recommendation in full[46], 10[47] have partly implemented it and 3[48] have not implemented it. One Member State has not provided any information[49]. There has been no significant change in implementation since last year's follow-up on this recommendation. This year, the Member States focused on providing information on their stage of implementation in 2018 and 2019. Several Member States referred to the upcoming transposition of the Union's Whistleblowing Directive by 17 December 2021[50]. Some Member States have already adopted legislation on whistleblowers in 2019[51].

In addition, the Member States were asked to promote systematic and timely cooperation between judicial and administrative authorities. Eighteen Member States have implemented this recommendation in full[52], 3[53] have partly implemented it and 3[54] have not implemented it. Three Member States have not provided information[55]. More Member States have fully implemented this recommendation since last year's partial or non-implementation[56]. The majority of Member States provided updated information on initiatives taken in 2019, with the role of AFCOS being more prominent than last year as a coordinator for cooperation in anti-fraud matters between different national authorities.

---

[41] Lithuania.

[42] Bulgaria, Czechia, Germany, Croatia, Greece, Italy, Cyprus, Latvia, Luxembourg, Hungary, Malta, Austria, Poland, Portugal and Romania.

[43] Belgium, Denmark, Estonia, Ireland, Spain, France, Slovenia, Slovakia, Finland and Sweden.

[44] The Netherlands.

[45] Lithuania.

[46] Bulgaria, Croatia, Greece, Italy, Latvia, Hungary, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia and Sweden.

[47] Belgium, Czechia, Denmark, Estonia, Ireland, Spain, France, Luxembourg, Slovenia and Finland.

[48] Germany, Cyprus and Austria.

[49] Lithuania.

[50] Germany, Ireland, Greece, Spain, France.

[51] Latvia and Slovakia.

[52] Belgium, Czechia, Greece, Spain, Croatia, Italy, Cyprus, Latvia, Luxembourg, Hungary, Malta, the Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia and Sweden.

[53] Belgium, Germany and Estonia.

[54] Denmark, Austria and Finland

[55] Ireland, France and Lithuania.

[56] Spain, Italy, Romania, Slovenia and the Netherlands

1. FOLLOW-UP BY RECOMMENDATION

METHODOLOGY AND THEMATIC ANALYSIS:

The following section provides a comprehensive overview of the implementation of each recommendation by the Member States and summarises the replies received for each recommendation. This section is divided in two sub-sections, one each on the recommendations related to the revenue and expenditure sides of the budget. Each recommendation is analysed first by providing results by the number of Member States that addressed each of the recommendations, and second by providing a summary of the most important details provided by Member States. For more details, readers are referred to the Member States' original replies which are reproduced under Section 2, 'Replies of Member States'.

1.1. REVENUE

The Commission provided the following questionnaire to the Member States with regard to addressing the first recommendation:

Q.1.1 *Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?*

Q.1.2 *Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?*

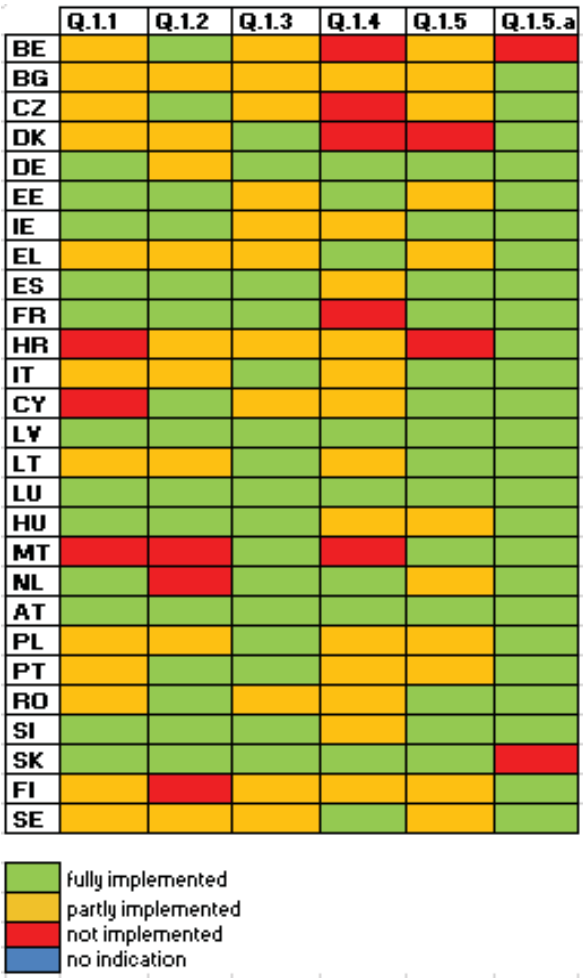
Q.1.3 *Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?*

Q.1.4 *Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?*

Q.1.5 *Have you ensured that ex post controls include verifications on traders' compliance with customs duty relief for low-value consignments?*

Q.1.5.a *Are authorised economic operators (AEOs) not excluded from such compliance checks?*

The table below represents the overall results of the implementation of each question corresponding to the Commission's recommendation.



1.1.1. CUSTOMS CONTROL STRATEGIES FOR CROSS-BORDER E-COMMERCE TRADE

The Member States were asked to provide information on whether they enhanced and enforced customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR). Twelve[57] Member States replied that they fully implement this question, 12[58] reported partial implementation and 3[59] have not implemented it.

[57] Germany, Estonia, Ireland, Spain, France, Latvia, Luxembourg, Hungary, the Netherlands, Austria, Slovenia and Slovakia.

[58] Belgium, Bulgaria, Czechia, Denmark, Greece, Italy, Lithuania, Poland, Portugal, Romania, Finland and Sweden.

Several Member States provided details in their replies (in summary)[60]:

Belgium reported that automatic selections occur in BE-gate but that quite a few operators are not there and BE-gate provides only limited selection options. It contains selection profiles for undervaluation and a random selection.

Bulgaria has no specific strategy targeting low-value consignments, as this has not been developed yet. However, the Customs Agency has developed and is implementing a strategy for controlling the customs value of imported goods, which covers low-value consignments.

The **Czech Customs Administration** uses focused risk profiles set for specific risky commodities under EUR 22. For consignments over EUR 22 and below EUR 150, electronic risk analysis is performed with no exceptions for AEOs. After January 2021, electronic risk analysis will be expanded on the consignments under EUR 22.

Denmark reported that the Danish Customs Agency has not adopted a separate control strategy within the area of cross-border e-commerce, but has stepped up its general focus in that area. For example, by carrying out control actions focusing on fraud and abuse related to the import of low-value consignments.

Estonia reported that about 20% of the postal and express consignments declared by individuals are sent for checking on the basis of a specifically created criterion. 100% of the consignments with low value, which are sent by C2C as gifts, are directed for checking.

Ireland reported that the Customs Division has various risk profiles in place for clearance and simplified declarations at national and local station level.

Greece reported that the operational plan of the IAPR includes quantitative targets for controls on e-commerce consignments. The measures taken include the introduction of a primary inspection prior to submission of the document, stepping up the means of control (X-rays, radiation detectors, sniffer dogs), etc.

Spain reported that risk profile updates take into account the new trends identified by the Customs Department of the Tax Agency.

France reported that items of negligible value are handled electronically and subject to checks. A risk analysis and investigations are carried out, aiming to detect value decreases.

Croatia reported that upgrades and improvements are planned for the new customs declaration (H7) which will be in production from 1 January 2021.

Italy indicated the memorandum stipulated by the Customs and Monopolies Agency that allows the operators to use a single customs tariff code in cases of declarations of goods under LVCR.

Cyprus is in the process of implementing a new system in 2022.

---

[59] Cyprus, Croatia and Malta.

[60] For more detailed information please see Section 2, 'Replies of Member States'.

Latvia explained that since November 2019, import customs declarations must be lodged for postal consignments. This functionality has been introduced in the national electronic customs data processing system. In addition, a strategy of control for postal consignments has been developed and put into practice.

Luxembourg reported that in addition to the general electronic customs clearance system and its rules engine applicable for electronic customs declarations, Customs deployed an IT solution (DAkOTA) especially dedicated to electronic risk analysis of structured pre-arrival consignment-level data related to low value shipments.

Hungary reported that with regard to cross-border e-commerce, the National Tax and Customs Administration (NTCA) drew up a separate strategy for 2020, taking into account the initial recommendation made in the PIF report for 2018. On 1 January 2021, an EU package will enter into force that will fundamentally change how small-value consignments are handled: VAT will have to be paid on them irrespective of the amount involved and, to ensure VAT is recovered, data will have to be submitted in advance.

The Netherlands reported that they started with a number of e-commerce companies to decrease the risk of low value consignments in close cooperation with the tax authorities.

The **Austrian** risk management approach in the field of low consignments is a combination of specific electronic risk profiles, risk profiles with a minimum control quota and focal control operations beside the electronic targeting system.

Poland's National Revenue Administration started work on optimising the clearance and control of e-commerce consignments in September 2018. A new customs clearance model was designed for postal traffic. A national analytical unit (Strategic Analysis Centre) is preparing the terms of reference and scope of operations for checking postal and courier consignments containing low-value goods.

Portugal reported that electronic declarations concerning e-commerce are covered by applied risk analysis parameters based on risk indicators/risk profiles.

Romania's General Directorate for Customs focused on the improvement of cooperation with public authorities, national and international organisations and other stakeholders in the field of fraud in cross-border e-commerce. It participates to the joint actions and national operations. It improves risk analysis and management to prevent the infringement of customs legal regulations on cross-border e-commerce and monthly monitors the results of the customs controls performed on postal/express courier consignments. Romania highlighted the development of an e-commerce strategy containing measures meant to improve the customs controls on postal/express courier consignments.

Slovakia reported on the procedure followed when goods are released into the free circulation, on entry of postal consignment where the declaration is fully completed and the customs officer considers the data to be relevant.

Finland: Finnish Customs has a control plan, 'Undervaluation through e-commerce'. For example, they analyse the operators in cross-border e-commerce trade.

Sweden: Swedish Customs is notified of all arriving low value consignments and the decision to release the goods is sent electronically from Swedish Customs to the designated UPU operator in Sweden.

1.1.2. TACKLING POTENTIAL ABUSE OF LOW-VALUE CONSIGNMENTS RELIEFS (LVCR)

The Member States were asked to provide information on whether they ensured that their electronic customs declaration system does not automatically apply claimed duty relief on: (a) goods with a declared intrinsic value above EUR 150, (b) commercial consignments declared as gifts and (c) goods ineligible for relief. Fifteen Member States[61] replied that they fully implement it and 10[62] reported partial implementation. Three Member States[63] have not implemented it.

Several Member States provided details in their replies (in summary)[64]:

Bulgaria replied that no customs declarations are filed electronically for consignments of a value up to BGN 30. For consignments with an intrinsic value of more than BGN 30 but less than EUR 150, a customs declaration is lodged by electronic means. As regards checking for potential abuses of relief from import duties and/or VAT on consignments of a value not exceeding EUR 150 and consignments of a value not exceeding EUR 45 sent from one individual to another and the financial risk criteria, there are plans to create risk profiles, which will be used to check compliance with the conditions for relief from customs duties and/or VAT and to monitor other criteria for identifying financial risks.

Denmark reported that their Customs Agency has implemented a 'lock' in the system to cause entries with a value above EUR 150 to fail if duty relief is claimed. Commercial consignments declared as gifts will fail unless it is stated to be a C2C shipment. Nothing was implemented concerning goods ineligible for relief.

Germany replied that there is a mechanism in the electronic customs clearance system that gives an indication to the user if the value of goods exceeds EUR 150. On declared gifts, only checks based on risk profiles are possible and have been implemented.

Estonia reported that when the duty relief is claimed on the declaration, the system checks if the use of this duty and VAT relief codes are justified. Also, 100% of declarations with low value and excise goods with declared low value are directed for checking.

Ireland explained the procedure in their e-customs declaration system for consignments of negligible value, for consignments where the customs value is less than EUR 45. Ireland does not have a built-in validation function to identify goods ineligible for relief, but a robust risk profiling system is in place.

Greece replied that in the case of goods not eligible for exemption, the electronic system does not automatically apply claimed customs duty relief. In the other two cases the claimed customs duty relief is not automatically applied until the special codes have been filled in.

[61] Belgium, Czechia, Estonia, Ireland, France, Spain, Cyprus, Latvia, Luxembourg, Hungary, Austria, Portugal, Romania, Slovenia and Slovakia.
[62] Bulgaria, Denmark, Germany, Greece, Croatia, Italy, Lithuania, Poland and Sweden.
[63] Malta, the Netherlands and Finland.
[64] For more detailed information please see Section 2, 'Replies of Member States'.

Greece notes that there are inherent difficulties in managing the customs declaration as regards identifying risks.

Spain reported that intrinsic value is not data included in the customs declarations. Based on the customs value, declared risk profiles are applied in order to detect incorrect declarations.

France replied that for trade flows (B2B and B2C) τhe French customs clearance system, Delta, is programmed to not grant relief from customs duties automatically for goods with a declared value lower than EUR 150. Automated checks have been put in place to ensure that relief is granted. An exemption is issued under two conditions. For non-commercial flows, the exemption from customs duties and VAT is fixed at EUR 45. The grant of the exemption is subject to verification under conditions.

Croatia: Customs declarations used for these kinds of duty relief are controlled under risk analysis profiles. There is no automatic applying of this duty relief. However, consignments under EUR 22 of value are not declared by a customs declaration.

Italy replied that the controls in the national IT system ensured non-automatically applied relief to low value shipments when the value presented to customs exceeds EUR 150. The identification of 'gifts' is not currently detectable as this indication is contained in box 44 in the free text subfield.

Latvia: The electronic customs data processing system does not allow the automatic application of claimed duty relief on consignments with a value exceeding EUR 150. A risk profile has been created to control goods declared as gifts and goods eligible for relief.

Luxembourg reported that Customs implemented both declaration processing and risk rules in their electronic customs clearance system in order to prevent the misuse of relief codes. AEOs are not excluded from these rules. Post-clearance controls by the audit unit also cover declarations declared under LVCR.

Cyprus replied that specifications (as rules) were created in the national application to prevent these cases from being submitted.

Hungary: Where the scope of items under Council Regulation (EC) No 1186/2009 setting up a Community system of reliefs from customs duty permitted, filters were incorporated into the customs data processing system and, in certain cases, systematic risk profiles were generated.

Malta replied that an upgrade in the Customs electronic system will be requested from their service provider to address this recommendation.

The Netherlands have not implemented this in the system because the customs value is not the same as the intrinsic value of a consignment.

Austria reported that there are procedures in the electronic system that check the submitted data to rule out the risks of submitting falsified documents. When necessary these are supported by specific risk profiles.

Poland introduced a rule triggering the need for the customs authority to check that the consignment's value does not exceed EUR 150. Goods declared as gifts are largely declared as postal consignments. The electronic customs declaration is not used in such cases. As

consignments of this type also benefit from VAT relief, they are declared in the form of a summary declaration. If the goods exceed EUR 150, the customs authority can refuse to accept a declaration claiming duty relief or accept the declaration and issue an assessment notice.

Portugal replied that the system for automatically processing import customs declarations does not allow the additional scheme code C07 to be declared if the value of the declared goods is in excess of EUR 150, nor does it allow code C08 to be declared if the value of the declared goods is in excess of EUR 45.

Romania implemented in 2018 a risk profile to impose the verification of the customs values declared for all the declarations containing the additional code C07.

Slovenia replied that their electronic customs declaration systems does not automatically apply claimed duty relief on goods with a value above EUR 150 and on declared gifts or on goods ineligible for relief. This is ensured by the risk analysis system and risk profiles.

Slovakia reported that customs clearance is done electronically but not all procedures for postal consignment are fully electronic and automatic.

Finland has no risk profile on this but is planning to set one up using random sampling.

Sweden: Low value consignments above SEK 2,500 are re-routed for post-clearance control in the system. The ones below SEK 2,500 are automatically cleared. For declared gifts with a value above SEK 500, the declaration is re-routed as well.

1.1.3. DETECTION OF POTENTIALLY UNDERVALUED OR INCORRECTLY DECLARED GOODS

Member States were asked to provide information on whether they have ensured that their electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly. Sixteen Member States[65] replied that they fully implement this recommendation and 11[66] reported partial implementation.

Several Member States provided details in their replies (in summary)[67]:

Bulgaria replied that risk profiles have now been established for checking the declared customs value of all goods falling within Chapters 61, 62, 63 and 64 of the Combined Nomenclature (CN) of the European Union, and they do not exclude low-value consignments.

Czechia noted that there are specific risk profiles for certain high risky commodities. On a global level, it is very difficult to set out a risk profile just for undervaluation, also because of the high volume of consignments per year.

Denmark reported that the Danish Customs Agency has implemented risk profiles that specifically select entries under the LVCR.

Estonia: 100% of the parcels with a declared value below EUR 22 are directed for checking.

Ireland has a significant number of profiles in place to target undervalued/incorrectly declared goods. Large-scale profiling, however, is subject to the proportionality test and impact assessment so as to avoid excessive and unnecessary profile hits at customs stations.

Greece: There are general and specific risk profiles as well as randomness profiles. However, lack of data hampers the effectiveness of targeting and controls.

Spain Risk profiles have been implemented for control in simplified customs declarations in low value consignments. 194 specific and 3 random risk profiles are in force since 2019. 72,400 customs declarations have been controlled thanks to these risk profiles.

The **French** customs authorities have put in place risk analysis and automated targeting of these flows, with a view to combating tax fraud. French Customs is in the process of recasting its targeting IT tools, in particular the RMS application, with a view to the use of the H7 declaration.

Croatia replied that no customs declaration is submitted for small-value consignments, under EUR 22, and no risk analysis profiles can be applied**.**

Cyprus: The risk analysis on low value goods is done manually by customs officers who select for control goods suspected to be undervalued. About 2% of the consignments that are selected for control are found to be undervalued.

[65] Denmark, Germany, Spain, France, Italy, Lithuania, Latvia, Luxembourg, Hungary, Malta, the Netherlands, Austria, Poland, Portugal, Slovenia and Slovakia.

[66] Belgium, Bulgaria, Czechia, Estonia, Ireland, Greece, Croatia, Cyprus, Romania, Finland and Sweden

[67] For more detailed information please see Section 2, 'Replies of Member States'.

Latvia replied that for postal consignments one of the main risks is undervaluation, and specific risk profiles were set up to tackle this. Risky companies and natural persons are profiled.

In **Luxembourg**, any available risk information on LVC is assessed and the necessary risk profiles are created whenever relevant.

Hungary: for low-value consignments, more risk profiles have been put in place since mid-2019. These check the duration of the conditions for customs and tax exemptions and, where necessary, systematically signal to the performer of the customs procedure what risk has been identified and what measures should be introduced to deal with the risk indicated. Since these profiles have been in effect, they have generated 804 hits, and action was taken in 160 of those cases.

Poland: Data entered in the declarations submitted for each consignment are sent from the operations system to the automated risk analysis system. This triggers an automated analysis, and if data are identified in the declaration that are risk criteria for the algorithm, a risk profile is activated, displaying a message with information on the risk and the scope and method of control.

Romania reported that identification of priorities within a risk area is based on information from bottom-up signals, new EU legislation and available resources. The risk analyses produced are risk profiles, info-risks, alerts etc.

Slovakia indicated that the risk profile warning checks all consignments for code C07 (low value shipments up to EUR 150) and those for which the code has been applied illegally, are regularly captured, as the value of the goods on the invoice was higher or the goods were incorrectly declared.

Sweden has risk profiles for random selection of declarations in the system. These declarations are evaluated and might undergo physical inspections.

1.1.4. SPECIFIC CONTROL MEASURES TO PREVENT ARTIFICIAL SPLITTING OF CONSIGNMENTS

Member States were asked to report whether there are any specific control measures in place to prevent artificial splitting of consignments with the aim of benefiting from duty relief. Nine Member States[68] replied that they fully implement this recommendation and 13[69] reported partial implementation. Five Member States[70] have not implemented it.

Several Member States provided details in their replies (in summary)[71]:

Bulgaria and Czechia replied that even though it is difficult to automate the process for screening consignments for artificial splitting with a view to benefiting from relief from duty, both are preparing measures and guidance in this matter for the future.

Estonia According to Article 37(4) of the Estonian Customs Act (https://www.riigiteataja.ee/en/eli/521012014009/consolide), the customs authorities may refuse to accept separate customs declarations for parts of a consignment upon import if the value of a declared part of the consignment does not exceed the tax exempt limit. For express consignments with a commercial purpose, the customs official checks manually if there is one single consignor, consignee and shipment document. For postal and express consignments declared by individuals, the system automatically checks the tracking number and if the same number has already been used it cannot be used again.

Spain also indicated that risk profiles are in force but splitting is very difficult to detect.

Croatia: In case of doubt, customs officers check internet orders to control if certain consignments are distributed deliberately for applying a duty relief.

Italy is planning to set up guidelines focused on the prevention for the artificial splitting of consignments.

Cyprus: During manual check of manifest report, customs officers are trying to detect shipments that may concern the same consignment. Such cases have very rarely been identified.

In **Latvia**, cases of artificial splitting are identified in the post-clearance process.

Hungary: Taking into account the findings of the judgment in case C-7/08 *Har Vaessen Douane Service BV* v *Staatssecretaris van Financien*), the customs data processing system does not permit preventive customs clearance in customs procedures requested under procedure 4000-C07.

The Netherlands has developed and implemented a monitoring tool.

---

[68] Germany, Estonia, Greece, Latvia, Luxembourg, the Netherlands, Austria, Slovakia and Sweden.

[69] Bulgaria, Ireland, Spain, Croatia, Italy, Cyprus, Hungary, Poland, Lithuania, Portugal, Romania, Slovenia and Finland.

[70] Belgium, Czechia, Denmark, France and Malta.

[71] For more detailed information please see Section 2, 'Replies of Member States'.

Poland: In the system handling import declarations, the declaration of exemption from customs duties of consignments up to a value equivalent to EUR 150 is flagged up so that the system operator checks that the value of the consignment does not exceed the equivalent of EUR 150. If the goods are found to exceed the equivalent of EUR 150, taking into account cases of artificial splitting, the customs authority can refuse to accept a declaration claiming duty relief (code C07) or accept the declaration and issue an assessment notice.

Portugal replied that measures to enable the potential identification of split consignments carried on different means of transport or under the cover of different transport documents are being examined for implementation. They are based on the analysis of the frequency associated with an operator and other data in the declaration. Such measures are likely to be introduced from next year (2021).

Romania: The General Directorate of Customs of the Ministry of Public Finances' National Agency for Fiscal Administration reported that the identification of priorities within a risk area is based on information from bottom-up signals, new legislation and available resources. For that purpose the risk analyses products used are risk profiles, Inforisks, alerts, etc. Those risk analysis products are mostly focused on LVCR, IPR etc. At the same time, the constant guidance provided to the customs officers by the headquarters specialised staff had in view this specific aspect of the possibility of fraudulent acts by means of splitting the consignments, aiming to benefit from duty relief.

Slovenia replied that the prevention of artificial splitting of consignments is ensured by means of risk profiles and risk analyses.

Slovakia: Consignments submitted are inspected by customs officers daily. For targeting consignments, customs officers check the consignor's country, repeating consignee, shape and size of consignment.

Finland replied that Customs have included one post-release audit in the control plan 2020 of express couriers, where they will examine also the splitting of consignments.

Sweden reported that artificial splitting is most common on exit declarations for customs warehousing. To prevent this, the customs clearance system for import does not accept the combination of procedure code 4071 with C07.

1.1.5. ENSURING THAT EX POST CONTROLS INCLUDE VERIFICATIONS OF TRADERS' COMPLIANCE ON LOW VALUE CONSIGNMENTS RELIEF

Member States were asked to provide information on whether they ensured that ex post controls include verifications on traders' compliance with customs duty relief for low-value consignments. Fourteen Member States [72] replied that they fully implement this recommendation and 11[73] reported partial implementation. Two Member States[74] have not implemented it.

Several Member States provided details in their replies (in summary)[75]:

In **Belgium**, ex post controls carried out are either the Court's Audit Policies and Standards (CAPs) or audits requested via proposals made by the risk management.

In **Bulgaria,** checks on low-value goods cover potential risks such as (i) the splitting of consignments into smaller consignments for the purpose of evading import duties, (ii) the relief from import duties of goods contained in consignments with an intrinsic value exceeding the BGN equivalent of € 150, (iii) incorrect tariff classification and/or incorrect declaration of the origin of imported goods for the purpose of circumventing various import measures resulting from EU policies, and (iv) invoices presented to the customs authorities when releasing low-value goods for free circulation that contain data diverging from those recorded in the company's accounts, e.g. quantity, description of the goods, invoice value, etc.

Czechia: Taking into account that consignees are mainly physical persons that have no obligation under Czech law to retain any evidence (invoices, etc.) it would be extremely difficult to prove a breach after the release of goods.

In **Ireland**, within their electronic 'Customs, Risk Intervention, Selection' programme, there are categories of risk rules within which the risks surrounding LVC are covered.

Greece replied that the recommendation is applied in full where an import document (declaration) is presented on the basis of a local risk analysis, whereas in cases where an 'oral' import declaration (non-statistical SAD) is presented the recommendation is partially implemented.

In **France**, national and local services rely on the expertise of the National Directorate for Customs Investigations and Intelligence to understand and block fraud patterns with a view also to establish monitoring methods and a suitable inspection policy. The main purpose of the surveys is to detect and sanction sub-assessments of value (from the first euro for VAT in the case of mail-order sales, and from EUR 150 onwards for customs duties).

---

[72] Germany, Ireland, Spain, France, Italy, Cyprus, Lithuania, Latvia, Luxembourg, Malta, Austria Romania, Slovenia and Slovakia.

[73] Belgium, Bulgaria, Czechia, Estonia, Greece, Hungary, the Netherlands, Poland, Portugal, Finland and Sweden.

[74] Denmark and Croatia.

[75] For more detailed information please see Section 2, 'Replies of Member States'.

Italy: Specific indications issued in 2017 in which, among other things, the selection of operators for PCA involves also who imports goods at risk of under-invoicing. In addition, the SIDDA IT procedure carried out a periodic detection of the anomalous values of certain parameters of customs declarations.

Cyprus: A big case of undervaluation was detected concerning the import of electronic cigarettes from China.

Latvia replied that it is not common practice to carry out post-clearance checks on LVC since the benefits are disproportionate to the amount of recovered duties. Controls for small-value shipments are carried out during customs clearance.

Hungary: Since post-release controls are imposed in the light of a preliminary risk analysis, low-value consignments regularly arriving in large numbers are examined as part of targeted inspections above and beyond the inspection plan, in cooperation with the risk analysis department.

The Netherlands has post-clearance audits at a number of companies.

Poland replied that operators holding customs exemptions for low-value consignments are therefore subject to the general rules of Union and national law governing the classification of operators for customs and tax control purposes. The department of the National Revenue Administration checking postal consignments introduced into the EU customs territory carries out the measures laid down in Chapter 3 of Title V of the Implementing Regulation and the controls provided for in Article 48 of the Union Customs Code.

Portugal reported that all economic operators are considered at the risk assessment stage with a view to selection for ex post controls. However, so far, no operators exhibiting potential risk characteristics leading to selection for ex post controls have been identified with regard to relief linked to low-value consignments.

Romania: The General Directorate of Customs of the Ministry of Public Finances' National Agency for Fiscal Administration reported that all territorial structures are obliged to include in the quarterly programmes of post-clearance controls the customs declarations that raise suspicions regarding the way of establishing the customs value.

Slovenia reported that the approach for selecting traders for ex post controls takes into account the frequency of parcel imports for particular consignor and/or consignee, the value of goods (low value) and the description/nature of goods.

Slovakia reported that the national post-release control plan for 2020 contains a specific focus on post-release checks on low-value shipments.

Finland reported that in 2020 they have one post-release audit of express couriers where Finnish Customs will control the courier's compliance with the LVCR.

Swedish Customs reported, among others, that it is working to correct declarations where procedure code C07 has been misused and to charge due duties to the declarant.

1.1.6. AUTHORISED ECONOMIC OPERATORS (AEOS)

Member States were asked to provide information on whether AEOs are excluded from compliance checks with customs duty relief for low-value consignments. As with last year's follow-up, the majority of the Member States[76] has implemented this recommendation in full. Two Member States[77] have not implemented it.

[76] Bulgaria, Czechia, Germany, Denmark, Estonia, Ireland, Greece, Spain, France, Croatia, Italy, Cyprus, Lithuania, Latvia, Luxembourg, Hungary, Malta, the Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Finland and Sweden.

[77] Belgium and Slovakia.

1.2. EXPENDITURE

This section summarises the Member States' replies. The Commission provided the following questionnaire to the Member States on the second recommendation:

Questionnaire:

1. National Anti-Fraud Strategies (NAFS)

Q.2.1 *Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?*

Q.2.1.a*. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?*

Q.2.1.b*. Has your national AFS taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?*

Q.2.1.c *Has your national AFS taken into account the need to structure the coordination between administrative and criminal checks and investigations?*

Q.2.1.d. *Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?*

2. Risk Analysis

Q.2.2.a *Has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?*

Q.2.2.b. *Can you share any results deriving from the use of findings from PIF reports in your fraud risk assessments?*

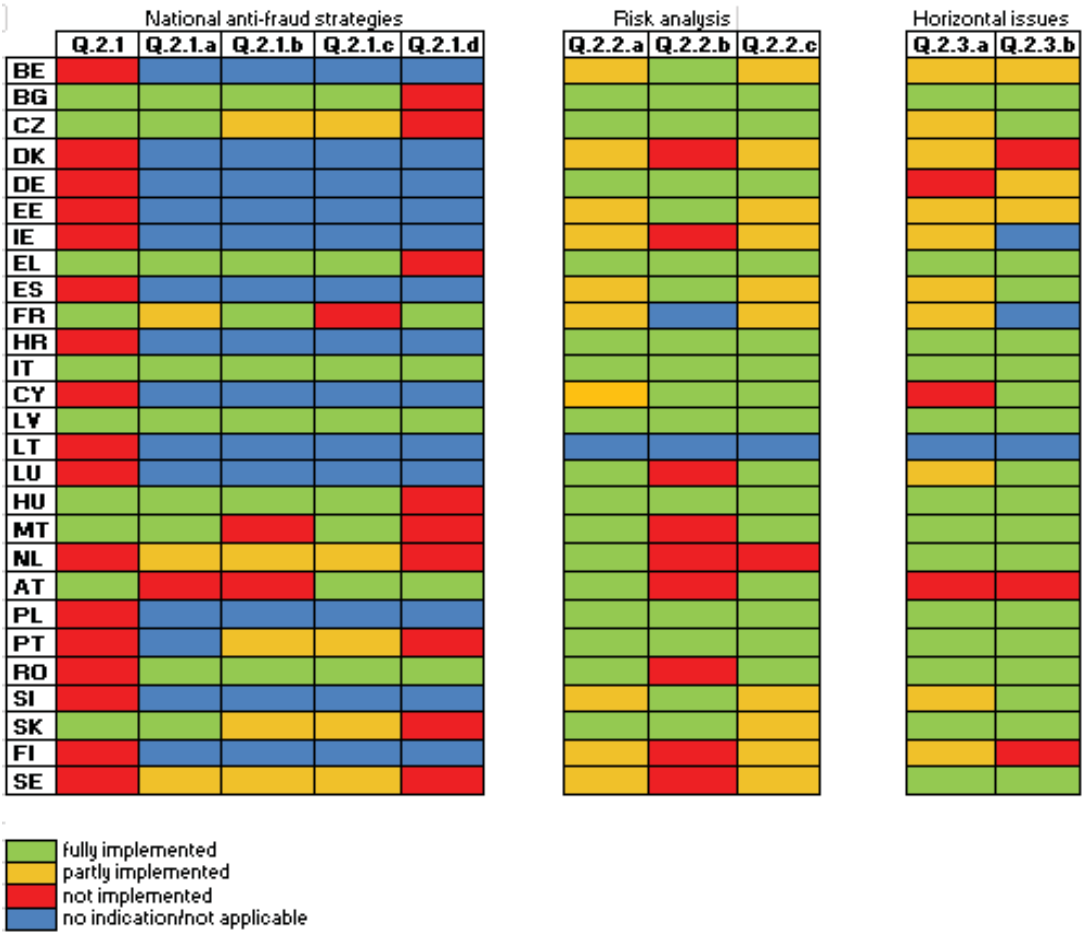
Q.2.2.c *Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?*

3. Horizontal Issues

Q.2.3.a. *Have you facilitated and assessed the spontaneous reporting of irregularities and strengthened the protection of whistle-blowers who are also a crucial source for investigative journalism?*

Q.2.3.b *Have you promoted systematic and timely cooperation between judicial and administrative authorities?*

The tables below show the overall results by question and Member State:



1.2.1. National Anti-fraud Strategies

The Member States were recommended to adopt national anti-fraud strategies (NAFS). These strategies should be developed in cooperation with all bodies and authorities which have a specific expertise and role in the protection of the EU's financial interests. Moreover, the strategies should take into account the risk analysis conclusions in the PIF report and the need to structure the coordination between administrative and criminal checks and investigations. The Member States were asked to share any results of the impact of their NAFS.

Ten Member States reported that they have adopted or updated a NAFS which they have communicated to the Commission (OLAF)[78]. 17 Member States have not adopted a NAFS[79], 4 are considering adopting one or are preparing a new NAFS not yet communicated to the Commission (OLAF)[80].

Nine Member States have fully developed their NAFS in cooperation with all bodies and authorities that have expertise in the area of the protection of the EU's financial interests, including law enforcement and prosecution services[81]. Three Member States have partly implemented this[82], 1 has not implemented it[83] and the recommendation was not applicable to the 14 remaining Member States[84].

Seven Member States developed their NAFS fully taking into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports[85]. Five Member States implemented this partially[86] whereas 2 have not implemented it[87]. This recommendation was not applicable to the 13 remaining Member States[88].

Eight Member States have developed a NAFS fully taking into account the need to structure the coordination between administrative and criminal checks and investigations[89], 5 have

[78] Bulgaria, Czechia, Greece, France, Italy, Latvia, Hungary, Malta, Austria and Slovakia.
[79] Belgium, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Luxembourg, Lithuania, Netherlands, Poland, Portugal, Romania, Slovenia, Finland, Sweden.
[80] Belgium, Spain, the Netherlands, Romania.
[81] Bulgaria, Czechia, Greece, Italy, Latvia, Hungary, Malta, Romania and Slovakia.
[82] France, the Netherlands, Sweden
[83] Austria.
[84] Belgium, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Lithuania, Luxembourg, Poland, Portugal, Slovenia, Finland.
[85] Bulgaria, Greece, Italy, Latvia, Hungary, Malta, Austria and Romania.
[86] Czechia, the Netherlands, Portugal, Slovakia and Sweden.
[87] Austria and Malta.
[88] Belgium, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Lithuania, Luxembourg, Poland, Sweden and Finland.
[89] Bulgaria, Greece, Italy, Latvia, Hungary, Malta, Austria and Romania.

implemented this partially[90] and 1 did not implement it[91]. This recommendation was not applicable to the 13 remaining Member States[92].

Five Member States made an assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests[93] and 9 did not[94].This recommendation was not applicable to the 13 remaining Member States[95].

Below are the Member States' replies (in summary)[96].

Belgium reported that their NAFS is under preparation. It should be adopted by the end of 2020.

Bulgaria's NAFS was adopted and communicated to the Commission/OLAF. It was drawn up with the cooperation of all bodies involved in the management and control of EU funds, including the Public Prosecutor's Office. It takes account of all European Union strategic and regulatory documents predating its adoption in 2014, including the PIF reports. In 2019 Bulgaria launched the process of drafting a national strategy for 2021-2027. In 2020 all the national authorities involved in the management and control of EU funds will continue working actively on the draft NAFS for 2021-2027. The new NAFS will be based in particular on risk analysis and will include the implementation of the recommendations of the Commission and the ECA, including the recommendations of the PIF reports.

Czechia has adopted a national strategy approved in Government Resolution No 535 dated 14 May 2008. In February 2020, an approval procedure for a second amendment was launched which reflects the developments in relevant legal acts as well as the recommendations of the ECA Special Report 6/2019. The national strategy has been drafted in consultation with all relevant bodies and authorities. To improve the effectiveness of cooperation in detecting and prosecuting irregularities and to define the framework for cooperation in reporting of irregularities concerning specific EU funds, agreements on the provision of information and cooperation were signed between the Central Contact Point (CCP) of AFCOS and the relevant ministries. Training by AFCOS is provided twice a year to relevant ministries to keep them updated with the latest developments in the PIF area.

Greece adopted a sectoral NAFS for cohesion policy accompanied by an action plan, submitted to OLAF on 5 May 2014 and updated in 2017. The Secretariat-General for Public Investments and the NSRF, the Financial Audit Committee (EDEL), the Financial Crime

[90] Czechia, the Netherlands, Portugal, Slovakia and Sweden.
[91] France.
[92] Belgium, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Lithuania, Luxembourg, Poland, Slovenia and Finland.
[93] France, Italy, Latvia, Austria and Romania.
[94] Bulgaria, Czechia, Greece, Hungary, Malta, the Netherlands, Portugal, Slovakia and Sweden.
[95] Belgium, Denmark, Germany, Estonia, Ireland, Spain, Croatia, Cyprus, Lithuania, Luxembourg, Poland, Slovenia and Finland.
[96] For more detailed information please see Section 2, 'Replies of Member States'.

Squad (SDOE), the National Anti-Corruption Coordinator and the General Inspector for Public Administration collaboratively developed the strategy and prepared the action plan up until the designation of the AFCOS, through constructive meetings and by providing texts and data. AFCOS is the link between the administrative authorities in the management and control system of the OPs of the NSRF 2014-2020 (CEPOL Objective) and the competent national authorities and bodies responsible for carrying out checks, but also for law enforcement and prosecution. The role of AFCOS in structural actions is provided for in the relevant institutional framework and is set out in detail with specific steps in the relevant procedures (and corresponding flow charts) of the MCS.

Spain: In 2019**,** the Advisory Council for the prevention and fight against fraud affecting the financial interests of the European Union created a Commission for the creation and follow-up of a National Antifraud Strategy in the field of the financial interests of the EU. Coordination of the NAFS is carried out by AFCOS (which holds its Secretariat), the General Public Prosecutor's Office, the National Police and Guardia Civil, all the managing authorities for Structural Funds, the Central Paying and Coordination Agency for agricultural funds, the Audit Authority, the Tax Agency, the Office for Asset Recovery, the State Treasury (Anti-money Laundering authority) and representatives of regional and local entities.

France's NAFS has not been developed involving the police and the prosecution service. The AFCOS has no investigative powers, and it did not consider that it was entitled to develop this strategy in coordination with the judicial and administrative authorities. However, any revision of the strategy will be developed in conjunction with the police and the judicial prosecutor's office. An impact of the NAFS to be shared is that the organisations that manage EU funds have better knowledge of the type of controls they need to prevent fraud.

Croatia has adopted two anti-fraud strategies so far. One covered 2010-2012 and the other 2014-2016, and both strategies were fully implemented. However, no new anti-fraud strategy has been adopted because of significant lack of human resources at the AFCOS service. At the same time, the AFCOS service has been faced with a constant rise in workload.

Italy gave an example of the impact of their NAFS for the programmes managed by the Agency for Territorial Cohesion: a fraud risk assessment team was established in the agency, which contributed to the formal adoption of risk assessment tools.

Latvia's first NAFS for 2017-2019 was adopted on January 16, 2017. The AFCOS started to work on new NAFS covering the period from 2020-2022. It is expected to be adopted in the first half of 2020 and afterwards communicated to OLAF. The AFCOS Council has been involved in drafting the NAFS, and it involved institutions including law enforcement and prosecution services. Concerning the impact of the NAFS, Latvia presented the campaign #FraudOff! To better understand the focus themes, AFCOS carries out a yearly study asking for public opinion on the level of fraud. According to a study carried out at beginning of 2019, overall confidence in the public administration in the prevention of fraud and corruption is very low, but compared to previous years, this indicator has increased (2017 -9%, 2018 -11%, 2019 -13%).

The preparation of a NAFS in **Luxembourg** is in progress. There is ongoing cooperation between national stakeholders and the competent Commission services. In addition, several managing authorities have already implemented internal policies describing the steps to follow in case of fraud detection. In cases of suspected fraud followed by an investigation, AFCOS is kept informed on the exchanges the managing authority has with OLAF and the Public Prosecutor's Office.

Hungary has had an anti-fraud strategy since 15 June 2015, which has been communicated to OLAF. The strategy was drawn up by the Prime Minister's Office, responsible for the use of EU funds that time, in collaboration with participants in the network of institutions involved in performing tasks related to development policy.

The **Maltese** NAFS tabled in Parliament in 2008 was also communicated to the Commission/OLAF. The strategy is currently in the process of being updated as necessary.

In **Romania,** a draft of the NAFS for the current PP was prepared, but it was not adopted in the reference period. The Romanian AFCOS is in the process of evaluating the updating of the draft strategy for the next programming period 2021-2027.

Slovakia: The Slovak NAFS was signed by the Head of the Government Office on 4 June 2019. The major novelty introduced in this updated NAFS is the new tasks for 2019-2020 defined in the action plan, which forms one of the Slovak NAFS' annexes. In addition, some of the tasks from the previous action plan have been moved to the main text of the Slovak NAFS as permanent tasks. The updated NAFS was sent to OLAF in December 2019. The NAFS was approved by a network of 21 partners representing the General Prosecutor's Office, the National Criminal Agency and the Ministry of Justice. The NAFS and the action plan contain various tasks on improving the coordination between administrative and criminal authorities. One of these is to set up a network of liaison officers at the level of the AFCOS network partners (these partners also include representatives of individual managing authorities, the General Prosecutor's Office, the National Criminal Agency and the Ministry of Justice) to enhance the effectiveness of operational cooperation in the area of protection of EU's financial interests in Slovakia.

Sweden reported that they have different, individual anti-fraud strategies for all authorities managing EU funds and to compile these strategies into one would not provide any added value.

1.2.2. RISK ANALYSIS

THE USE OF IT TOOLS

The Member States were asked to provide information on whether risk analysis has been strengthened to detect irregularities and fraud, including using IT tools such as ARACHNE. 16 Member States have fully implemented this recommendation [97], 10 have partly implemented it[98] and 1 has not provided information[99].

Below are the Member States' replies (in summary)[100]:

In **Belgium,** the MA of Wallonia ERDF Programme still uses ARACHNE, and the Brussels ERDF MA has boosted its control of the result indicators provided by the coordinators of financed projects by implementing a new systematic control procedure.

Bulgaria reported that the MA of operational programmes financed by EU structural funds regulate access to ARACHNE through administrative orders specifying the names and positions of those with access to ARACHNE. Bulgaria provided detailed information of the use of ARACHNE set out in the following chapters of the manuals of the MA for individual programmes: 1. the chapter on risk management and the related risk control, 2. the chapter on financial management, 3. the chapter describing the steps for providing grants, and 4. the chapter on irregularities.

Czechia set up a risk management system at the level of operational programmes, which consists of systematic identification, evaluation, management and reporting of all significant risks, within which due attention is paid to the identification and management of fraud risk. The MA has established the Register of Fraud Indicators and the Register of Complaints from Information Systems. Data from both records are entered through the set of risk factors into the interim risk analysis on projects. The interim risk analysis on the projects from which the control plans are generated is carried out on the basis of risk factors (e.g. risk factor Presence on the list of the 10 most risky projects in Arachne, Presence of the applicant on the list of risk entities and the state of affairs, increased risk of fraud). Information on detected fraud indicators is shared across the MA's departments, which leads to general awareness and gives individual employees experience of fraud indicators and their search. Furthermore, in the MA self-assessment process, all representatives of departments at the level of directors are acquainted with all cases of detected fraud indicators during the reporting period. At present, data mining from Arachne as part of administrative check is being tested.

The **Danish** Business Authority carries out data analysis, including cross-analysis and risk-based sampling in each reporting period for all projects. In autumn 2014, the MA carried out

[97] Bulgaria, Czechia, Germany, Greece, Croatia, Italy, Latvia, Luxembourg, Hungary, Malta, the Netherlands, Austria, Poland, Portugal, Romania and Slovakia.
[98] Belgium, Denmark, Estonia, Ireland, Spain, France, Cyprus, Slovenia, Finland and Sweden.
[99] Lithuania.
[100] For more detailed information please see Section 2, 'Replies of Member States'.

an initial test of Arachne, but has reservations about to compliance with data protection rules when using the tool. The Agricultural Agency obtained external expertise from Deloitte to expand and structure their risk profile with regard to project support (NON-AIACS). With regard to ARACHNE, the agency continuously monitors and evaluates the experience of other authorities and Member States with the tool.

In **Ireland**, further steps were taken in 2019 by the ERDF Managing Authorities to implement ARACHNE. This included the first batch imports of live ERDF data from the Irish eCohesion system to ARACHNE and training for the ERDF managing authority and certifying authority staff. This was provided by the Commission's ARACHNE team in May 2019 and led to further development work by the managing authorities to align eCohesion reports with the ARACHNE system requirements.

Greece makes use of the following tools: 1) the Integrated Information System (IIS), which is the central management tool and the means of electronic data exchange among all the authorities/bodies involved; 2) the State Aid Management Information System (PSKE) and the State Aid Cumulating System (SACS); 3) The Irregularities Management System (IMS) and 4) the Commission's Fraud Risk Assessment Tool (developed by DG REGIO). Greece provided a description on how risk analysis is conducted, and on the reporting of irregularities via IMS. The Directorate for Financial Control, Audit and Cooperatives selects the undertakings to be audited as part of the annual audit programme by applying a risk analysis methodology. The managing authority of the Fisheries and Maritime OP has taken measures which are recorded in the Fraud Risk Assessment Tool concerning the detection of irregularities, and the relevant OLAF Guidelines are also implemented.

Italy has established a Fraud Risk Assessment Task Force and a Checks Quality Review Task Force in addition to implementing ARACHNE.

Cyprus replied that among other factors, their risk analysis process takes into account the results of previous years' verifications and on-the-spot checks, the frequency of the errors identified in each project, the nature of the projects, nature of beneficiaries and type of expenditure. This information is consolidated at fund level and is taken into account at the sampling process. Therefore, high-risk areas are more likely to be selected for verifications or on-the-spot checks. Additionally, the 'Summary of Errors' (SoE), which is annually submitted to the EC through the submission of the accounts, is used to document all the irregularities identified through several verifications, including cases which may be excluded from reporting because these have been detected before the submission of the payment claim. The SoE of previous year is taken into account in order to determine the verification strategy in the next year. Further to the above, a new development is the access to the electronic platform of the Department of Registrar of Companies and Official Receiver has been provided to authorised officers of the Verifications and Certification Directorate, through which companies' information can been identified. This tool allows authorised users to identify any relationships between corporate beneficiaries and/or its representatives (e.g. Directors) and shareholders, which can be used to assess whether there is any potential conflict of interest when awarding contracts to beneficiaries funded by ESIF funds.

In **Latvia**, the Ministry of Finance, MA for Structural Funds, makes use of ARACHNE among other available databases. The Ministry of Agriculture's Rural Support Service uses its IT system tools including a list of risk clients, links to other external systems, area satellite imagery and atypical case studies.

Hungary has installed ARACHNE in every MA. How actively Arachne is used depends on the group of beneficiaries a MA has. MAs which typically cooperate with the budgetary institutions do not use ARACHNE, as the FAIR EUPR fraud prevention functionality provides them with sufficient information. This special functionality was developed in the section of the Hungarian Development Policy Database and Information System (FAIR) dealing with Union support. Its aim is to prevent fraud and abuses and detect it early (the 'fraud prevention functionality'). The functionality is being constantly improved in the light of emerging needs: in 2018, it was expanded with a question about indicators. According to the model protocol for irregularity procedures issued by the Coordination Body, cases of irregularities registered as suspected fraud must be recorded separately, so they can also be filtered using the FAIR EUPR irregularity module.

The Netherlands reported that after several pilot projects in previous years on the use of ARACHNE, this year ARACHNE is fully operational. To this end, project data was exchanged with ARACHNE. This has not led to detection of fraud.

In **Poland,** as regards cohesion policy, successive measures have been taken to reinforce risk analysis aimed at detecting different kinds of irregularities and fraud. This is done using IT tools that simplify work and step up action in the selected fields. A 'Cross Checks' IT application is being developed for the purpose of identifying cases of double financing of expenditure incurred by beneficiaries implementing projects co-financed by Union funds.

Portugal's Inspectorate-General for Finance - Audit Authority (IGF - AA) uses ARACHNE, which has been instrumental in getting the other national authorities to start 'feeding' and using it.

Romania provided examples from various authorities. For instance, the Ministry of European Funds often detects irregularities and in some instances fraud as a direct consequence of using ARACHNE together with other internal methods of verification and control.

In **Slovenia**, ARACHNE is mainly used for development and cohesion policy. However, it is used in combination with information provided in different national computer applications (for example as provided by the Commission for the Prevention of Corruption called Erar, application Gwin, application e-credit). Also, the MAs use risk analysis for selection of the projects to be checked on the spot. ARACHNE is not always the best tool for the Slovenian situation (ARACHNE is very useful tool when dealing with a non-Slovenian provider).

MAs use risk analysis also for selection of the projects to be checked (by MA and IB) on the spot.

Slovakia reported that the Ministry of Environment, the Ministry of Agriculture and Rural Development, the Ministry of Education, Science, Research and Sport, the Ministry of Interior and the Antimonopoly Office are making full use of the ARACHNE tool, in combination with other useful IT tools for the detection of irregularities. The Ministry of Education provided an example. The irregularities recorded under OP II (Operational Programme research & innovation) were identified based on media coverage of calls for applications for a non-repayable financial contribution to support and irregularities resulting from the investigation of the National Criminal Agency. The case is being prosecuted for the offence of damaging the EU's financial interests in parallel with the crime of machinations in public procurement and public auctions.

THE USE OF PIF REPORTS' FINDINGS IN FRAUD RISK ASSESSMENTS

The Member States were asked to share any results deriving from the use of the PIF Reports' findings in their fraud risk assessments. 16 Member States shared their results[101], and 9 did not have any results to report[102]. One Member State has not provided information.[103]

Below are the Member States' replies (in summary)[104]:

Belgium's ERDF Wallonia reported (a) the signing by the beneficiaries of a declaration of absence of conflicts of interest in public procurement contracts and (b) the continuous use of the ARACHNE tool.

Bulgaria: In 2019, the Ministry of the Interior's AFCOS Directorate carried out administrative checks on the reporting and management of reports of fraud and irregularities at the State Fund for Agriculture. The inspections resulted in reports in which, following analysis of the problem areas identified, the AFCOS Directorate made recommendations aiming to make the fight against irregularities and fraud affecting the EU's financial interests more effective. For its part, the State Fund for Agriculture has taken the steps necessary to implement the recommendations made by the AFCOS Directorate.

Czechia: In the checklists for on-the-spot checks, the MA has added questions about ARACHNE concerning public procurements and contracts or concerning eligibility and efficiency of expenditures. In 2019, the MA's self-assessment and the regular evaluation of the implementation of measures of the strategy for combating fraud and corruption within the drawing of funds of the common strategic framework in 2014-2020 were carried out. The internal anti-corruption programme for 2018-2020 was updated in 2018. Cooperation with the police in the case of fraud has been gradually intensified by written, electronic or phone communication. A special department was created for communication with the Czech Police.

Estonia reported improved risk analyses in order to find cumulative supports to the same land cadastres despite different applicants, with the goal of finding artificially created applicants in the area of rural development.

Greece: The Directorate for Financial Control, Audit and Cooperatives of the Ministry of Rural Development and Food shared two results: (a) scoring and mapping as many risk parameters as possible, in order to see that the selection of undertakings best ensures the effectiveness of measures to prevent and detect irregularities; (b) ensuring the quality of ex post checks and cross-checks of the commercial documents of those entities receiving or making payments and directly or indirectly related to the system of financing by the EAGF, or

[101] Belgium, Bulgaria, Czechia, Germany, Estonia, Greece, Croatia, Italy, Cyprus, Latvia, Luxembourg, Hungary, Poland, Portugal, Slovenia and Slovakia.
[102] Denmark, Ireland, Luxembourg, Malta, the Netherlands, Austria, Romania, Finland and Sweden.
[103] Lithuania.
[104] For more detailed information please see Section 2, 'Replies of Member States'.

their representatives, in accordance with Regulation (EU) No 1306/2013 of the European Parliament and of the Council.

Italy: The use of findings from PIF enabled improvements in the control system.

Cyprus: Risk assessment has been incorporated into all administrative and on-the-spot procedures undertaken by responsible bodies involved in programmes under shared management in the areas of cohesion policy, fisheries and aid to the most deprived. Risk assessment methodologies, for example, are incorporated into systems for selecting procurement procedures in order to perform administrative verifications of the legality and regularity of the tender notice, evaluation and assignment procedures. Risk analysis is also used to select transactions for verification of payment claims submitted by beneficiaries with a large number of supporting documents, or during on-the-spot controls for measures with a large number of final recipients. Risk analysis incorporates data on the nature of beneficiaries, the nature of projects and the type of expenditure involved, based on ex ante assessment of the associated risk to each category and incorporating results of previous verifications and audits. Additionally, through the preparation of SoE and typology of errors (common typology of errors), we can identify the frequency of errors in each type of error and target the high-risk areas in order to proceed with enhanced control testing and verifications in the next year.

Latvia: the Rural Support Service has identified individual cases that have allowed the detection of irregularities and the prevention of undue payments.

Hungary: The use of a specially designed fraud prevention functionality in the part of Hungary's IT system (FAIR) dealing with EU funds (EUPR) is ongoing; this interface provides information on every project, with the aim first and foremost of preventing fraud and abuse and enabling early detection. The use of ARACHNE is continuous in investigations where it provides information in addition to that provided by the national IT system (such as on ownership relationships, for instance).

Poland: Since 2016, the staff of the Agency for Restructuring and Modernisation of Agriculture, in its capacity as the Paying Agency, have been made more aware of fraud by: (1) the introduction of a list of red flags for the purpose of raising the awareness of staff involved in all stages of the administrative and control cycle of anomalies (signs) that could warrant suspicions of fraud; (2) annual analysis of the risk of fraud aimed at identifying risk areas, evaluating the effectiveness of the control mechanisms deployed and, in specific cases, introducing new control mechanisms to reduce to a minimum the risk of fraud in respect of financial support granted by the Agency; and (3) training on fraud for Agency staff.

Romania: The Ministry of European Funds reported that the MA has not used any results of findings from PIF Reports, mainly due to the fact that the findings presented in the report describe, among other things, various rules (e.g. new rules adopted to reduce VAT fraud), different operational measures adopted by several Member States on expenditure to raise awareness, a collection of main achievements regarding detection of fraud and irregularities

by some Member States etc., whereas the purpose of fraud risk assessment was intended to be a useful tool for self-evaluation, based on which the MA could easily identify new possible risks, following a careful consideration of the status quo of each internal structure within the MA. However, the MA fully complies with the requirements stipulated at Chapter 9.9.2 of the 2018 final PIF report issued by OLAF. For example, the MA has an anti-fraud policy in place and, at the same time, provides useful information and actively participates (when requested) to meetings in order to strengthen the efforts to create and properly implement the national anti-fraud strategy. Some irregularities and all cases of fraud identified by the MA are managed in very close collaboration with institutions that are directly responsible for criminal checks and investigations (e.g. DLAF, National Anticorruption Directorate etc.). The MA takes into consideration all viable external sources such as whistleblowers and tips from media. The information received form this kind of sources is carefully analysed and afterwards cross-examined by competent bodies, without disclosing the identity of the person. The protection of personal data of the source is guaranteed by internal procedures and other specific national and EU regulations. Given the examples provided above, The Fight against Fraud Department (RO AFCOS) took into account the conclusions from the previous PIF reports concerning the fraud risk assessment of every authority by introducing a specific objective in the draft national anti-fraud strategy.

Slovenia: Cooperation with the State Attorney's Office, better information with the IB, better cooperation with the IB, early detection of fraud upon improved checklists, improved system performance and consequently fewer corrections.

Slovakia: Provided examples (findings and measures) by the Ministry of Interior, the Ministry of Agriculture and the Ministry of Environment. An indicative example is the one given by the Ministry of Agriculture and Rural Development. In line with the zero-tolerance approach to fraud, the managing authority for the programmes Interreg SK-CZ and SK-AT prepared and published an anti-fraud policy document. Managing authorities use risk analysis to identify the most vulnerable areas of fraud. Managing authorities also use IT tools such as ARACHNE, the IT monitoring system ITMS2014+ and a system to protect whistleblowers.

The Member States had been recommended to further exploit the potential of risk analysis, tailoring the approach to different types of expenditure. 15 Member States have fully implemented this recommendation[105], 10 have partly implemented it[106] and 1 has not implemented it[107]. One Member State has not provided information[108].

Below are the Member States' replies (in summary)[109]:

Belgium's ERDF Brussels-Capital region's MA is considering carrying out an extensive control of compliance by project coordinators with State aid legislation in 2020.

Bulgaria provided information about risk analysis carried out by the MA for the Structural Funds, the MA for Agricultural Funds and the Audit Authority. Bulgaria provided a best practice example of 2019: eight officials from the State Fund for Agriculture and one from the Ministry of the Interior's AFCOS Directorate underwent training in countering irregularities and fraud at Croatia's Agriculture, Fisheries and Rural Development Agency. The purpose of the visit was to share best practices from the measures developed and implemented by Croatia and Bulgaria to combat fraud and irregularities in the management of EU agricultural funds.

Czechia described the MA's monitoring of the occurrence of fraud indicators during 1) the review in the process of project approval/before awarding the grant, and 2) the control in the project implementation process. On 1 January 2019, the risk analyses were divided into risk analysis for individual projects and risk analysis for simplified projects, which are in some respects specific and the originally set of risk scale factors were not adequate.

Denmark: The Danish Business Authority indicated the use of OBS lists. There is and probably always will be potential for smarter use of data, particularly where there is a very large and growing volume of data. The Danish Agricultural Agency has carried out a risk analysis of project support, divided into market organisations, schemes with standard costs and schemes with two tenders. The aim was to identify and rank risks in relation to the Agency's current fraud prevention frameworks. The Danish Fisheries Agency reported that in 2018 and 2019 they reviewed their administrative fundament and case management. This has led to the detection of cases of suspected fraud. The areas with the highest risk of fraud have been stating the correct level of expenditure, and maintaining eligibility after completing an operation. These findings have led to updates and alterations in the legislation and their case-handling procedures. The measures taken have been risk based, however not on the basis of ARACHNE but on national IT tools and especially case-handling procedures.

[105] Bulgaria, Czechia, Germany, Greece, Croatia, Italy, Cyprus, Latvia, Luxembourg, Hungary, Malta, Austria, Poland, Portugal and Romania.

[106] Belgium, Denmark, Estonia, Ireland, Spain, France, Slovenia, Slovakia, Finland and Sweden.

[107] The Netherlands.

[108] Lithuania.

[109] For more detailed information please see Section 2, 'Replies of Member States'.

Ireland: The ERDF MA had been carrying out (mid-2017-early 2018) a risk assessment of each intermediate body (IB) submitting a declaration of expenditure to the MS. The MA is now in the process of reviewing these and are also undertaking risk analysis on those IBs that are progressing from expenditure to declaration stage.

Greece provided examples of risk analysis exploitation by EYTHY (the Special Institutional Support Service), EDEL (the Financial Audit Committee) and the Directorate dealing with Agricultural Funds. EYTHY explained that the methodology for risk assessment of operations/beneficiaries applied under the MCS for planning the spot checks on non-State aid operations includes risk factors/indicators which take account of different types of expenditure.

France: The audit authority notes that the irregularities relate mainly to the same subjects: public procurement, State aid and eligibility of expenditure. The audit authority bases its risk analysis on all the irregularities declared in the SYNERGIE information system. This enables it to map the risks at national level but also at regional level, taking into account all audits (operation audits and system audits) and to better target the audit plan and supervision of audits according to the risks highlighted in each region.

Cyprus: Information regarding staff involved in co-financed projects has been incorporated into the MIS used for the management of four shared management programmes covering the areas of cohesion policy, fisheries and aid to the most deprived. Staff cost has been assessed as a high-risk area for fraud during the fraud risk self-assessment exercise undertaken by the responsible authorities. The information in the MIS will be extracted from reports in order to identify trends and used in the framework of administrative and on-the-spot controls. This function is in progress and is being gradually implemented.

Luxembourg: In 2016, following a fraud discovery, the MA for FEAGA and FEADER created the 'Procedure and Special Investigations' whose mission is to prevent fraud cases. Before that, a guidance note for premium managers to prevent fraud in the agricultural sector had been created. The reason behind it was a scam which was discovered in 2013 following an internal administrative audit. Following that incident, the Ministry of Agriculture fundamentally reviewed its external and internal control systems. An alert system has also been set up to detect facts that may indicate fraud or attempted fraud. In case of INTERREG, the expenditure is always 100% controlled, but the manual of the program insists on paying particular attention to the staff cost and to external expertise, in particular to the services that require respect for public procurement procedures. A risk chart has also been created and is updated on a biannual basis (last time in 2018). For ESPON, the risk approach has been tailored since it mainly focuses on public procurement. Specific provisions where included in the programme implementation guidelines for the single beneficiary.

Hungary: The MAs identify and assess the risk of fraud on the basis of the EGESIF_14-0021-00 guidance document published by the Commission, for which the Hungarian authorities have drawn up methodological guidance.

Poland: As regards cohesion policy, the sampling of expenditure and projects for control is based on risk analysis. The assumptions underlying the analysis are set out in the annual

control plans drawn up for each operational programme for a given accounting year. MAs also apply the risk analysis advocated in the Commission's guidelines.

Romania: The MA for Operational Programme Administrative Capacity identified that, as a result of the use of the fraud risk assessment tool recommended by the Commission, it is necessary to use the ARACHNE instrument in a specific manner regarding public procurement expenses and to use a different approach of the instrument as far as the process of evaluating financing operations is concerned.

Slovakia: The Ministry of Interior identified insufficient strategy for improving professional skills in the area of fraud prevention and detection.

Sweden: Typically the Swedish authorities managing EU funds only deal with one type of expenditure rather than several types. The annual assessment is carried out with the purpose of identifying new risks, evaluating actions, etc.

1.2.3. CROSS-CUTTING ISSUES

The questions concerning the assessment of spontaneous irregularities, strengthening whistleblower protection and enhancing cooperation between judicial and administrative authorities are repeated from last year. Last year, the results showed that about half the Member States implemented the recommendation related to whistleblowers. On the promotion of systematic and timely cooperation between judicial and administrative authorities, just about half of the Member States implemented this last year. This year's follow-up aims at shedding more light into the Member States' actions concerning the implementation of this recommendation.

ASSESSING THE SPONTANEOUS REPORTING OF IRREGULARITIES AND STRENGTHENING THE PROTECTION OF WHISTLEBLOWERS

The Member States were recommended by the Commission to facilitate and assess the spontaneous reporting of potential irregularities and strengthen the protection of whistleblowers, who are also a crucial source for investigative journalism. 13 Member States have implemented this recommendation in full[110], 10[111] have partly implemented it and 3[112] have not implemented it. One Member State has not provided any information[113].

Several Member States provided details of their actions taken in 2018/2019 (in summary)[114]:

Belgium: In its regional policy declaration (2019-2024), the Walloon Government has committed to recognising whistleblower status by ensuring the protection of any official who,

[110] Bulgaria, Croatia, Greece, Italy, Latvia, Hungary, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia and Sweden.
[111] Belgium, Czechia, Denmark, Estonia, Ireland, Spain, France, Luxembourg, Slovenia and Finland.
[112] Germany, Cyprus and Austria.
[113] Lithuania.
[114] For more detailed information please see Section 2, 'Replies of Member States'.

in good faith, reports criminal behaviour within his/her administration and to extending application of this status across regional and local public services. This process is ongoing.

Bulgaria provided detailed information about the reporting system established within the managing authorities of operational programmes' websites with regard to structural funds. They provided an example: in 2019 two reports concerning suspected fraud under one of the operational programmes by the beneficiary of two different projects led to a total of seven on-the-spot checks by the managing authority's irregularities officers: one on the beneficiary, four on its partners in the two projects, and, following a second report concerning one of the projects, two simultaneous on the-spot checks on the equipment supplied and the two partners. The files relating to the checks carried out under the two reports were sent to the Public Prosecutor's Office for follow-up.

Czechia: There is no special legal act for the protection of whistleblowers in Czechia yet, but an act is currently under preparation. In general, there are special websites, email addresses and/or phone lines at each ministry for whistleblowers. Complaints from third parties relating to the implementation of projects from the ESIF are recorded and investigated and dealt with as suspected irregularities. Depending on the nature of the complaint, it is determined whether it will be verified by an administrative or on-site inspection or whether a criminal complaint may be filed. An example of findings detected during on-the-spot check that have been performed because of information received from informants is an irregularity concerning childcare facilities.

The **Danish Business Authority**, the MA for the ERDF and ESF, has specified further guidance for whistleblowers in the anti-fraud policy. Last year they launched a new whistleblower scheme, which is based on a web form solution allowing the possibility to report anonymously.

In **Germany**, there is no comprehensive legal provision to protect whistleblowers. Following the entry into force of Directive (EU) 2019/1937, there is a need of transposition for both the private and public sectors. The Federal Government is working on the necessary measures to ensure that the Directive is implemented by December 2021.

Estonia: In 2019, a draft bill was presented to the Parliament, which among other amendments also strengthens the protection of people who report breaches of anti-money laundering measures.

Ireland: The EU Whistleblowing Directive, which must be transposed by 17 December 2021, will require changes to Ireland's legislation in this area.

Greece: The establishment of a modern institutional framework for the protection of whistleblowers is an action of the National Anti-Corruption Action Plan (NACAP). Greece is in the process of adopting new rules for the protection of witnesses, which were published in the Official Journal of the EU on 26.11.2019 (Directive 2019/1937).

Spain: In line with what was reported last year, more managing authorities/intermediate bodies and paying agencies have adopted the confidential channel established by AFCOS and have fulfilled its recommendations in order to facilitate the spontaneous reporting of

irregularities and fraud affecting the financial interests of the EU. The number of allegations received through the reporting channel was higher in 2019 than in 2018. With regard to the protection of whistleblowers, the legislative proposal (reported last year) was ultimately not adopted because of the general elections in Spain in 2019. Now that the Directive (EU) 2019/1937 has been adopted, Spain will initiate the process for its transposition.

France also reported that it will transpose Directive EU 2019/1937 of 23 October 2019 on the protection of persons who report breaches of EU law.

Croatia: As regards the spontaneous reporting of irregularities and in case of suspected fraud, alerts are forwarded to the State Attorney's Office and the Ministry of Interior by AFCOS. Nonetheless, the AFCOS Service cannot measure the real effect of its work (i.e. coordination activities) because it relies on written observations submitted by competent management and control system bodies (irregularity reporting system bodies) and it does not check the substance of the case. The Irregularity Management System (IMS) has eight cases where irregularities have been established based on the information received from informants, out of which two cases relate to suspected fraud. The Act on the Protection of Whistleblowers was adopted on February 8, 2019 and came into force on July 1, 2019 (OG 17/2019).

Cyprus replied that the whistleblowers regulation is yet to be released by the Parliament.

Latvia: The Whistleblower Protection Law entered into force on May 1 2019. The Rural Support service received two alarm reports which were evaluated but the facts were not confirmed. Also, the focus theme for 2019 in social campaign #FraudOff! Was 'Reporting culture'. A reporting tool was created where individuals can report about different irregularities (www.atkrapies.lv).

Poland: In 1 January-31 December 2019, the paying agency and implementing bodies initiated 1,182 investigations into reports of irregularities and fraud. In 2019 there were 102 fewer investigations than in 2018. On 9 January 2020 the situation with regard to reports on suspected irregularities received by the paying agency was as follows: 1) no irregularities were found in 378 cases; 2) irregularities were found in 59 cases; 3) proceedings are ongoing in 572 cases; and 4) reports were left unexamined in 173 cases.

Portugal: A specific section for whistleblowers is available on the website of the Inspectorate-General for Finance - Audit Authority (https://www.igf.gov.pt/paginas-participacao-civica/nova-participacao.aspx).

Romania provided examples from various authorities' experience. The Ministry of European Funds approved the system procedure for reporting irregularities and the protection of people who complain or notice irregularities. The MA for Operational Programme Administrative Capacity had as source of detection of irregularities/frauds whistleblowers or mass media reports, which are currently being treated as being in the suspicion phase and undergoing specialised checks/investigations.

Slovenia's Government Office for Development and European Cohesion Policy reported that guidance is currently being prepared concerning lobbying. Whistleblower standards will also be included. In the case of consent, the guidance will be published on the MA website and thus will be binding for all IM bodies.

Slovakia adopted in January 2019 an Act on the protection of whistleblowers, on anti-social activity and on amendments to certain acts. This Act also creates a new Office for the protection of whistleblowers with new competencies in this field, as an independent state administration body. Information was also provided by various government departments on different measures taken to implement the recommendation.

In **Finland,** the possibility for anonymous reporting was established for structural funds.

Sweden reported that one of the largest newspapers (*Dagens Nyheter*) has written several articles about suspected irregularities in the Swedish ESF Council. The newspaper was able to get access to all documents thanks to the Swedish Public Access to Information and Secrecy Act.

Cooperation Between Judicial and Administrative Authorities

The Member States were recommended to promote systematic and timely cooperation between judicial and administrative authorities. Eighteen Member States have implemented this recommendation in full[115], 3[116] have partly implemented it and 3[117] have not implemented it. Three Member States have not provided information[118].

Several Member States provided details of their actions taken in 2018/2019 (in summary)[119]:

Bulgaria: In 2019, three instances of suspected fraud were reported to the Public Prosecutor's Office under only one of the operational programmes. The prosecutions service has followed up all three reports and pre-trial investigations are currently under way. Most cases of irregularities are detected prior to payment, but where fraud is found to have resulted in the payment of irregular expenditure, managing authorities of operational programmes take measures to recover public funds from the dishonest beneficiaries. As regards the agricultural funds, the State Fund for Agriculture works closely with representatives of the Ministry of the Interior's AFCOS Directorate, the Ministry of Interior's specialised investigative bodies, the managing authorities of operational programmes financed by EU Structural Funds and the Public Prosecutor's Office. The Audit Authority sent 14 final audit reports containing suspicions of fraud identified during the audit checks to the Public Prosecutor's Office for appropriate follow-up.

Czechia reiterated that cooperation between individual administrative and judicial authorities and individual procedures are regulated in the relevant chapters of the Operational Manual.

[115] Belgium, Czechia, Greece, Spain, Croatia, Italy, Cyprus, Latvia, Luxembourg, Hungary, Malta, the Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia and Sweden.
[116] Belgium, Germany and Estonia.
[117] Denmark, Austria and Finland.
[118] Ireland, France, and Lithuania.
[119] For more detailed information please see Section 2, 'Replies of Member States'.

Estonia reported that regular meetings with different related bodies (the Environment Agency, Competition Authority and other investigative bodies) take place to discuss the risky projects/support measures to prevent fraud and other problems.

Greece, as part of the procedure for setting up a mechanism for monitoring criminal cases, and in accordance with the circulars issued by the Supreme Court Public Prosecutor's Office (2/2018 and 2a/2018), collects case statistics from the whole country every 4 months on the progress of all pending cases relating to the prosecution of corruption, financial crime and money laundering. The data are collected anonymised, and include all ongoing cases of fraud against the financial interests of the European Union. The data are brought to the attention of the administrative authorities (Ministry of Justice, National Authority for Transparency – AFCOS). At the same time, AFCOS, in cooperation with UNODC, is working on creating a standardised statistical data collection system, which will be fully in line with the country's current obligations, to provide input to international organisations and bodies, including OLAF.

In **Spain,** the AFCOS has been working together with Guardia Civil and National Police to formalise the corresponding cooperation agreements with those entities, covering issues such as operative support and exchange of information, mutual technical advice, strategic cooperation and training. The AFCOS has also been working with the State Attorney's Office to formalise a procedure for the transmission of punctual information regarding the initiation, follow-up and closure of judicial (criminal) proceedings which affect the EU's financial interests.

Croatia: A regulation on the institutional framework of the system for combating irregularities and fraud has been adopted. This regulation defines AFCOS as a system comprised of (1) administrative authorities (irregularity reporting system bodies/management and control system bodies); (2) law enforcement and prosecution authorities, as well as authorities which have a specific expertise (AFCOS network); and (3) a coordinating authority (AFCOS service). The decision on the AFCOS network has been adopted. Protocols on cooperation have been signed with the State Attorney's Office, the Ministry of Interior and the Audit Authority. Meetings have been organised between administrative authorities (irregularity reporting system bodies/management and control system bodies) and law enforcement and prosecution authorities, or authorities which have a specific expertise (AFCOS network) in cases where administrative authorities need expert opinion (advice) from law enforcement and prosecution authorities, or authorities which have a specific expertise.

Cyprus: Enhanced cooperation between judicial and administrative authorities exists in cases of detected irregularities which may result in a suspicion of fraud or established fraud. Any other types of irregularities are handled within administrative authorities. The Legal Department of the Cyprus Government and specifically the European Union Law Section of the Attorney General together with the Cyprus Police work closely with AFCOS. Especially where an economic operator resists in any control (performed either by OLAF or VCD or IB), and authorities other than administrative are required in order to be able to proceed with the on-the-spot checks, the three authorities liaise between them and if required the check is

performed at the economic operator premises in the presence of police. In other cases, a Bank Judicial Disclosure Order was necessary in order for OLAF to be able to obtain any necessary information from the economic operator, and this was achieved through close collaboration between the Legal Department, Cyprus Police and OLAF.

In **France,** the Ministry of Justice met OLAF in October 2019 and requested to be informed of the judicial recommendations issued by the Office to the French courts. Such information could help to improve the follow-up procedures and cooperation with OLAF. Systematic and regular promotion of such cooperation will be explored when the anti-fraud strategy is next revised.

Latvia: In 2019, several interinstitutional meetings were organised between administrative bodies in EU funds and law enforcement bodies working on criminal cases. Those meetings and exchange of information are essential, not only to take appropriate administrative measures in projects, but to assist investigation in general. There are training programmes regarding cooperation structure which are designed in close collaboration between investigation authorities and administrative institutions. The aim of this training is to help institutions better understand each other's work and to find the best ways to cooperate on daily basis. These kinds of educational activities were carried out in 2018 and 2019.

Luxembourg: In March 2019, a member of Luxembourg's AFCOS and one prosecutor covering OLAF related issues jointly attended a conference in Bucharest called 'EU Anti-Fraud Partners' Meeting'. The latter was organised by Romania's Fight against Fraud Department – DLAF. The aim of the event was to provide a basis for exchanging information, experience and best practices on EU anti-fraud issues, especially in the context of the future cooperation between Member States, OLAF and EPPO. Further, in November 2019, an EU Conference on investigating frauds and corruption affecting the financial interests of the European Union in Bucharest was attended by a representative of Luxembourg's Inspectorate General of Finances.

In **Portugal**, in addition to the Inspectorate General for Finance (IGF) making its own resources available, the Audit Authority participates in training sessions (Lisbon and Porto) aimed at public prosecutors on 'Fraud in obtaining subsidies'.

In **Romania**, cooperation with judicial and administrative authorities is governed by national legislation and internal working procedures. The Managing Authority for the Regional Operational Programmes reported that there are requests for information and documents from the National Anticorruption Directorate, to which the Ministry of Public Works, Development and Administration responds promptly, but also requests formulated by the MPWDA to the NAD regarding the state of the NAD investigations. The information is requested for the correct updating and reporting of cases of suspected fraud. There is no collaboration protocol concluded between MPWDA and NAD, but there are two collaboration protocols concluded between MPWDA and The Fight against Fraud Department and the National Agency for Integrity, respectively, regarding the exchange of information. The General Directorate for European Territorial Cooperation – Ministry of European Funds reported that there are requests for information and documents from the National Anticorruption Directorate, to

which the Ministry of Public Works, Development and Administration responds promptly. Also, the MPWDA requests NAD information on the status of investigations in order to update suspicion cases. There is no collaboration protocol concluded between the MPWDA and NAD, but there are two collaboration protocols concluded between the MPWDA and The Fight against Fraud Department and the National Agency for Integrity, respectively, regarding the exchange of information.

Slovenia: An annual meeting between the EU Cohesion Policy Department and the State Attorney's Office at the end of 2019 took place to discuss outstanding issues and how the cooperation between the two bodies could be strengthened. The cooperation was found to be exemplary and positive for both sides. The result is also a table of all open procedures/cases where the ECP is the subject/legal basis, as well as sending a few examples of open cases with brief descriptions of what stage/status they are in.

Slovakia: Organised training sessions in 2018 for AFCOS Network partners on the protection of the EU's financial interests. In 2018, the Public Procurement Office started to deepen cooperation with key central state administration and judicial bodies on the basis of signed cooperation agreements.

2. REPLIES OF MEMBER STATES

2.1. REVENUE

Revenue fraud through the undervaluation of goods imported in the EU will remain a threat in the coming years. OLAF's investigations on the undervaluation of textiles and shoes imported from China demonstrated that fraudsters will use any loopholes and that large-scale fraud can pay off. The digitalisation of the global economy and new economic models like e-commerce are rapidly shifting cross-border trade from a few large/bulk shipments to a large number of low-value and small shipments. Cross-border e-commerce trade of goods poses risks for the EU's financial interests and for the Member States.

A particular risk is the abuse of the low-value consignment reliefs by: (i) undervaluing e-commerce trade goods; (ii) splitting consignments so that they fall below the relief threshold (EUR 150); (iii) importing commercial consignments declared as gifts; or (iv) importing goods ineligible for the relief.

Growing e-commerce requires that Member States' adapt their customs control strategies to strike the right balance between trade facilitation/simplification and protecting the EU's financial interests.

A flexible combination of different controls is therefore pivotal to close any loophole exploited by fraudsters and to enable customs to successfully respond to different economic models applied through technology (like e-commerce) and to effectively protect the EU's financial interests while permitting trade facilitation and simplification.[120]

[120] See PIF report 2018 p.30 https://ec.europa.eu/anti-fraud/about-us/reports/communities-reports_en

BE	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?☒YES, partly implementing the recommendation** *Automatic selections occur in Be-gate but:* • *quite a few operators are not in Be-gate;* • *Be-gate provides only limited selection options (for instance, FRC cannot be fully implemented).* *It contains selections profiles for undervaluation and also a random selection.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief**? ☒YES, fully implementing the recommendation Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly? ☒YES, partly implementing the recommendation *Automatic selections occur in Be-gate but:* • *quite a few operators are not in Be-gate;* • *Be-gate provides only limited selection options (for instance, FRC cannot be fully implemented).* *It contains selections profiles for undervaluation and also a random selection.* Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?☒NO *There are no clear guidelines yet as to what should be done with the control results should a control take place.* Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments? ☒YES, partly implementing the recommendation *The ex-post controls carried out are either CAPs or audits. These types of controls are requested via proposals made by Risk Management. Operations are therefore only able to carry out the CAPs/Audits requested.* Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?☒NO

BG

Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)? ☒ YES, partly implementing the recommendation

No specific strategy specifically targeting low-value consignments has been developed yet. The Customs Agency has developed and is implementing a strategy for controlling the customs value of imported goods, which covers low-value consignments. Furthermore, on the Customs Agency's intranet, newsletters have been published concerning relief from import duties and/or VAT on the release for free circulation of consignments of negligible value (up to EUR 150) or consignments sent from one private individual to another (up to EUR 45).

Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief? ☒ YES, partly implementing the recommendation

Article 23(1) of Council Regulation (EC) No 1186/2009 of 16 November 2009 setting up a Community system of reliefs from customs duty currently grants relief from import duties for goods with an intrinsic value not exceeding EUR 150 per consignment dispatched from third countries, provided the goods contained in those consignments are not subject to prohibitions and restrictions. Article 58(14)(1) of the VAT Act (ZDDS) grants VAT relief for goods imported under the duty-free arrangements, provided the total value of the goods does not exceed BGN 30. In this context, no customs declarations are filed electronically for consignments of a value up to BGN 30. Such consignments are deemed to have been declared for release for free circulation under Article 141 of Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code. The act deemed to be a customs declaration is the consignment's presentation to customs pursuant to Article 139 of Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, provided that the data required are accepted by the customs authorities.
In such cases, the risk analysis and the verification of compliance with the conditions for relief from customs duties and VAT are carried out manually using the data from the paper version. Note, however, that data which are not received electronically are often of poor quality, which limits the risk analysis that can be carried out. For consignments with an intrinsic value of more than BGN 30 but less than EUR 150, a customs declaration is lodged by electronic means. Relief from import duty is granted by entering the code CO7 'Consignments of negligible value' in data element 1/11 'Additional procedure'. For consignments sent by one private individual to another containing goods of a value not exceeding EUR 45, relief from import duty and VAT is granted, in accordance with Article 25 of Regulation (EC) No 1186/2009 and Article 58(14)(2) of the VAT Act, by entering code CO8 'Consignments sent from one private individual to another' in data element 1/11 'Additional procedure'. The postal operator Balgarski Poshti EAD currently uses the Customs Information System for imports to lodge customs declarations for release for free circulation containing the reduced data set for consignments of a value not exceeding EUR 1000. Despite the reduced data set, risk analysis is carried out on the basis of the information provided and no restrictions are applied to consignments for which the code CO7 or CO8 figures in data element 1/11. The other operators, including express couriers, use standard customs declarations to declare low-value consignments. Risk analysis and other additional checks are carried out using a full data set. There are no exceptions to the risk analysis for them either.
Those customs declarations, including those for low-value consignments, therefore undergo risk analysis, including analysis of the financial risks. Steps have been taken to configure automatic controls to check whether goods for which relief is sought by entering code CO7 'Consignments of negligible value' or code CO8 'Consignments sent from one private individual to another' in data element 1/11 'Additional procedure' qualify for relief from import duties. Pursuant to the Director of the Customs Agency's Order No ZAM-147 of 3 February 2020, the release version of the Customs Information System for imports is to undergo acceptance testing from 5 to 14 February 2020. During that period automatic controls are to be configured for checking those conditions, thereby ensuring compliance with the recommendation that the system should not automatically apply claimed duty relief to goods with the declared intrinsic value above EUR 150 or consignments sent from one private individual to another with a value of more than EUR 45. As regards checking for potential abuses of relief from import duties and/or VAT on consignments containing goods of a value not exceeding EUR 150 and consignments of a value not exceeding EUR 45 sent from one private individual to another and the financial risk criteria, there are plans to create risk profiles, which will be used to check compliance with the conditions for relief from customs duties and/or VAT and to monitor other criteria for identifying financial risks. Steps have also been taken to update the Customs Information System for imports in the light of amendments to the VAT rules applicable to e-commerce.

Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly? ☒ YES, partly implementing the recommendation

Risk profiles have now been established for checking the declared customs value of all goods falling within Chapters 61, 62, 63 and 64 of the Combined Nomenclature (CN) of the European Union, and they do not exclude low-value consignments. Identical risk profiles have also been created for certain plastic products, toys, light fittings, handbags, articles of a kind normally carried in the pocket and certain devices used with telecommunications apparatus.

CZ	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?** ☒YES, partly implementing the recommendation *Czech Customs Administration uses focused risk profiles, set for specific risky commodities under 22 €, performed by competent officers on the control spot of the Customs offices. For the consignment over 22 € and below 150 € electronic risk analysis is performed, based on general and specific electronic risk profiles. There are no exceptions for AEOs. After 1 January 2021, electronic risk analysis will be expanded also on the consignments under 22 €.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (wc) on goods ineligible for relief**? ☒YES, fully implementing the recommendation **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?** ☒YES, partly implementing the recommendation *For certain high risky commodities (such as clothes, shoes, electronics, automotive parts) there are specific risk profiles set out. On global level, it is very difficult to set out a risk profile just for undervaluation, also because of high volume of consignments per year (there is about 30 millions of consignments forwarded to the Czech Republic just by the Czech Post). Certain risk profiles are still being prepared and discussed for future development.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒NO *While it is very difficult to set out a specific control measure which can be focused on artificial splitting of consignments, Czech Customs Administration is still discussing and preparing such measure which will be directly focused on that. At present time, controls and measures, which are focusing on such case, are made mainly on random basis in connection with other risks. It is like this because until today majority of customs declarations for consignment are under 22 € and are declared orally or by any other act. For the future, when obligation of electronic customs declaration comes into force, special measure will be set also for the e-commerce goods.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments**? ☒YES, partly implementing the recommendation *Czech Customs Administration does not exclude low value consignments from its post release controls, but in case that the impact of such control has a low economic meaning and volume of the consignment is very high (about 30 million of separate parcels), priorities of post release controls are in different field. Taking into account the fact, that that consignees are mainly physicals persons, that have no obligation (according to Czech law) to hold any evidence (invoices, orders and so on), it would be extremely difficult to prove any breach after the release of goods.* Q. **1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** ☒YES, fully implementing the recommendation. *AEOs are not excluded from any kind of compliance checks, including e-commerce and low value consignments trade.*

DK	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?**☒YES, partly implementing the recommendation *The Danish Customs Agency has for the time being not adopted a separate control strategy within the area of cross-border e-commerce. However, the Danish Customs Agency has enhanced its general focus on cross-border e-commerce, and therefore also on the potential abuse of low-value consignments reliefs (LVCR). To this end, the Danish Customs Agency e.g. carries out control actions focusing on fraud and abuse related to the import of low-value consignments.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?**☒YES, partly implementing the recommendation *The Danish Customs Agency has implemented a "lock" in the system, which causes entries with a value above EUR 150 to fail if duty relief is claimed. Besides, a "lock" has been implemented in the system, which means that commercial consignments declared as gifts will fail unless it is stated to be a shipment from private to private. The Danish Customs Agency has not implemented anything concerning goods that are ineligible for relief.* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?** ☒YES, fully implementing the recommendation *The Danish Customs Agency has implemented risk profiles that specifically select entries under the LVCR for control with focus on undervaluation and misclassification.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒NO *The Danish Customs Agency has not initiated control measures with a specific focus on preventing artificial splitting of consignments.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☒NO *The Danish Customs Agency: For the time being, post release control (ex-post control) does not include verifications on traders' compliance with customs duty relief for low-value consignments. However, the Danish Customs Agency has ongoing discussions with the designated postal operator concerning customs related issues, such as the handling of low-value consignments.* **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** *The Danish Customs Agency do not perform the compliance checks described in Q. 1.5. However, when AEOs dealing with low-value consignments get their certification, the operators' processes are reviewed.*

DE	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?**☒YES, fully implementing the recommendation **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?** *(a) the declared intrinsic value above EUR 150 and (c) on goods ineligible for relief? ☒YES, partly implementing the recommendation* *In the electronic customs clearance system (ATLAS) exists a mechanism that gives an indication to the user if the value of the goods exceeds EUR 150. The user decides whether to stop the process or not.* *(b) on commercial consignments declared as gifts ☒YES, partly implementing the recommendation* *As long as the commercial nature of a good is not foreseen as an indicator in the customs declaration, the information can only be derived from the content of the consignor / consignee data (i.e. indication of a legal entity like "GmbH" or "AG" which does not unambiguously indicate the commercial nature). Therefore only checks based on risk profiles are possible and have been implemented.* *(c) on goods ineligible for relief? ☒YES, fully implementing the recommendation* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?** ☒YES, fully implementing the recommendation **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?** ☒YES, fully implementing the recommendation **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☒YES, fully implementing the recommendation **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** ☒YES, fully implementing the recommendation

EE	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?**☐YES, fully implementing the recommendation *Our control strategy is based on the efficient risk analysis. Approximately 20% of the postal and express consignments declared by private persons are sent for checking on the basis of a specially created risk criterion. For postal and express consignments with commercial purpose a random selection criterion is applied. 100% of the consignments having a low value, which are sent from C2C as gifts, are directed for checking.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?** ☐YES, fully implementing the recommendation a)*when the duty relief is claimed on the declaration, then the system checks if the use of this duty and VAT relief codes are justified;* *b)100% of the declarations with the declared low value (examples, samples) are directed for checking* *c)100% of the declarations (excise goods) with the declared low value (examples, samples) are directed for checking* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?** ☐YES, partly implementing the recommendation *In the postal company, the employee performs the initial check (manual risk analysis) of the items and if there is a doubt, directs it to customs clearance. The postal workers are trained by the customs.* *For postal and express consignments having a commercial purpose a random selection criterion is applied. 100% of the parcels with the declared value below EUR 22.00 are directed for checking.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☐YES, fully implementing the recommendation *According to article 37, § 4 of the Estonian Customs Act (https://www.riigiteataja.ee/en/eli/521012014009/consolide): (4) The customs authorities may refuse to accept separate customs declarations for parts of a consignment upon import if the value of a declared part of the consignment does not exceed the tax exempt limit. For express consignments with a commercial purpose the customs official checks manually if there is one single consignor, consignee and shipment document. For postal and express consignments declared by private persons the system checks automatically the tracking number and if the same number has already been used, then it cannot be used again.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☐YES, partly implementing the recommendation Customs officials check regularly the quality of the declarations submitted by couriers and customs agents. **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?**☐YES, fully implementing the recommendation **-** *All AEOs are covered with the same risk criteria as non-AEOs and are also included in the quality control checks.*

IE	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?**☒YES, fully implementing the recommendation Response: *To enhance and enforce our Customs Control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs , Customs Division has various risk profiles in place for Clearance and Simplified Declarations at National and local station level. The profiles target all or a selection of the following factors on declarations: Amount, Origin, Net/Gross Mass, Express Carriers, Consignors and item level. Profiles are created in proportion to the overall risk and are monitored regularly for effectiveness.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?**☒YES, fully implementing the recommendation *Part (a): In our e-customs declaration system (AEP) code CO7 is input in Box 37b for consignments of negligible value where the intrinsic value is less than €150. However, if the intrinsic value input is above €150 the appropriate rate of duty will be charged accordingly.* *Part (b): In our AEP system code CO8 is input in Box 37b for consignments where the customs value is less than €45. However, if the customs value input is above the threshold with C08 in Box 37b the appropriate rate of duty will be charged accordingly.* *Part (c): Although we do not have a built-in validation function within our system to identify goods ineligible for relief, we have we have a robust risk profiling system in place and in addition to this declarations can be subject random inspection or to a verification audit as part of our ongoing post clearance inspection programme.* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly***?*☒YES, partly implementing the recommendation *We have specific risk profiles which systematically target potentially undervalued or incorrectly declared goods. As noted in our response to Q1.1 our profiles target a range of risk factors and we also target consignments randomly. Additionally, we have created profiles specifically targeting each commodity code in Chapters 61-64 of the CN (textiles and footwear). While we have a significant amount of profiles in place to target undervalued/incorrectly declared goods, large scale profiling is subject to the proportionality test and impact assessment so as to avoid excessive and unnecessary profile hits at our customs stations.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒YES, partly implementing the recommendation *We acknowledge that the issue raises serious risks from a fiscal perspective and we are exploring the best avenues of approach with a view to full implementation by the date of the introduction of IOSS on the 01/01/21.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☒YES, fully implementing the recommendation *IE has a post clearance programmes unit in place that has planning policy in accordance with identified priorities with relevant monitoring and controls in place, utilising available risk analysis and risk assessment tools. Within our electronic Customs Risk, Intervention, Selection Programme (CRISP), there are categories of risk rules within which the risks surrounding low-value consignments are covered.* *For example*: *1. Use of C07 code in B37 (Consignments of negligible value) for Multi Item SAD where C07 code is present in some but not all items and B46 Stat Value is greater than 150 euro.* *2. Traders with 10 or more SADs within a 4 month period using the same CN code with code C07 in box 37, possible misuse of this code to avoid duty.* **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** ☒YES, fully implementing the recommendation *Response: AEOs are not excluded from any post clearance interventions including risks identified in CRISP.*

EL	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?** ☒YES, partly implementing the recommendation *IAPR (Independent Authority for Public Revenue) – CUSTOMS: The Operational Plan of the IAPR includes quantitative targets for controls on e-commerce consignments. The measures taken include the introduction of a primary inspection prior to submission of the document, stepping up the means of control (x-rays, radiation detectors, sniffer dogs), etc.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?**☒YES, partly implementing the recommendation *IAPR (Independent Authority for Public Revenue) – CUSTOMS: In the case of goods not eligible for exemption, the electronic system does not automatically apply claimed customs duty relief. In the other two cases the claimed customs duty relief is not automatically applied, but only after the special codes have been filled in. For a more comprehensive approach, customs officers make a primary inspection before the electronic submission of the document, where infringements are often found (e.g. false declaration as a gift/low value, etc.). Please note that there are inherent difficulties in managing the customs declaration as regards identifying risks.* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?**☒YES, partly implementing the recommendation *IAPR (Independent Authority for Public Revenue) – CUSTOMS: There are general and specific risk profiles as well as randomness profiles. However, lack of data hampers the effectiveness of targeting and controls.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒YES, fully implementing the recommendation **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☒YES, partly implementing the recommendation *IAPR (Independent Authority for Public Revenue) – CUSTOMS: The recommendation is applied in full where an import document (declaration) is presented on the basis of a local risk analysis, whereas in cases where an 'oral' import declaration (non-statistical SAD) is presented the recommendation is partially implemented.* **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?**☒YES, fully implementing the recommendation

ES	Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?☒YES, fully implementing the recommendation *Risk profiles are updated taken in account the new trends identified by the Customs Department of the Spanish Tax Agency.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?** ☒YES, fully implementing the recommendation *Intrinsic value is not a data included in the customs declarations. Traders have to request the exemption including the corresponding codes in box 37.2 of customs declaration. Based on the customs value (and its adjustments) declared risk profiles are applied in order to detect incorrect declarations.* **Q. 1.3 Have you ensured that your ECS systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?**☒YES, fully implementing the recommendation *Risk profiles have been implemented for control in Simplified Customs Declarations in low value consignments. 194 specific and 3 random risk profiles have been in force in 2019. 72.400 customs declarations have been controlled due to this 197 risk profiles.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒YES, partly implementing the recommendation *Risk profiles are in force, but splitting is very difficult to detect. In case of detection, proper measures will be applied.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☒YES, fully implementing the recommendation *Regular exchange of data with courier companies and controls over final consignees.* Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?☒YES, fully implementing the recommendation *AEO are not excluded of controls.*

FR

Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?☒YES, fully

Low value consignments are handled electronically and are subject to checks. Risk analysis and investigations are carried out in order to detect undervaluation. This is to ensure that duty relief for goods with a value lower than EUR 150 has been lawfully granted (see answers below).

Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?☒YES, fully implementing the recommendation.

A/ For trade flows (B2B and B2C*): The French customs clearance system, Delta, is programmed to not grant relief from customs duties automatically for goods with a declared value lower than EUR 150. Automated checks have been put in place to ensure duty relief is granted appropriately. Duty relief is granted if the following two conditions are met:*

- *the trader must include an additional Community code (C07) in the customs declaration;*
- *this code generates an automated admissibility check in Delta to ensure that the value declared in box 42 of the customs declaration does not exceed EUR 150.*

B/ For non-trade flows (C2C): *VAT and duty-free entry are set at EUR 45. Duty relief is granted subject to the verification of the following two conditions:*

- *the trader must include an additional Community code (C08) in the customs declaration, used to declare C2C goods with a value lower than EUR 45;*
- *this code generates an automatic admissibility check in Delta to ensure that the value declared in box 42 of the SAD does not exceed EUR 45.*

If the codes are not provided, the goods are taxed and the amount of duties and tax are calculated automatically.

Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?☒YES, fully implementing the recommendation

The French customs authorities have effectively implemented risk analysis and automated targeting for these flows in order to combat tax evasion.

Risk analysis and automated targeting: We have defined risk criteria and have integrated risk profiles into our IT system. Indeed, the French customs clearance system Delta is connected to an application specifically dedicated to automated risk analysis (RMS or Risk Management System). Risk profiles can be integrated at local, regional or national levels. These profiles are aimed in particular at detecting customs undervaluation.

Combatting undervaluation is a priority for the French customs authorities. The objective is both the recovery of customs duties and the recovery of VAT. The French customs authorities are currently updating their targeting IT tools, particularly the RMS application, so that the H7 declaration can be used. It has been decided that checks on flows cleared through customs using the H7 declaration will be carried out following an automated risk analysis but also by random selection.

Random selection checks during customs clearance: The French customs authorities have decided to continue to give staff the possibility of randomly checking declared goods, although automated selection is the only way to check declarations lodged for conventional freight.

Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?☒NO

This type of risk is not taken into account by our customs clearance IT system (Delta), but will however be dealt with as part of the update to our declaration targeting IT system (RMS).

HR	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?**☒NO *Upgrades and improvements are planned for the new customs declaration (H7) which will be in production from 1 January 2021. By then, the current system cannot be upgraded.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?**☒YES, partly implementing the recommendation *Customs declarations used for declaring these kinds of duty relieves are under control by risk analysis profiles. There is no automatic applying of this duty relief. However, consignments under 22 EUR of value are not declared by a customs declaration.* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?**☒YES, partly implementing the recommendation *No customs declaration is submitted for small value consignments, under 22 EUR, and no risk analysis profiles can be applied.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒YES, partly implementing the recommendation *I case of a doubt, customs officers check Internet orders to control if certain consignments are distributed deliberately for applying a duty relief.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☒NO **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** ☒YES, fully implementing the recommendation

IT

Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?☒YES, partly implementing the recommendation

The answer "yes partly" is justified by the "Memorandum" stipulated by the Customs and Monopolies Agency that allows the operators to use a single customs tariff code in cases of declarations of goods under LVCR.Anyway, specific risk profiles have been set up within the system of selecting customs declarations carried by the main operators in the sector. A working group has been set up, coordinated between central and local offices, dedicated to carrying out specific analyses, monitoring and controls at express and postal courier companies.

Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?☒YES, partly implementing the recommendation

Given that the concept of intrinsic value expressed in the application is not applicable as it refers to future developments in the field of ecommerce; the following is represented:In application of the recommendation 1 first point the controls currently implemented in the national IT system ensured not automatically apply claimed relief to low value shipments when the value presented to customs exceeds € 150;The identification of "gift" shipments is not currently detectable by the IT system as this indication is contained in box 44 in the free text subfield.

Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?☒YES, fully implementing the recommendation

The Customs Declaration Selection System provides both risk profiles with specific indicators and random selections.

Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?☒YES, partly implementing the recommendation

Regarding the traffic B to B the answer is "yes partially" because we are planning to set up guidelines focused on the prevention of the artificial splitting of consignments. These guidelines are going to be issued taking into account the specific future results of the IOSS working group of the DG Taxud. Regarding the traffic B to C the answer is "no" due to the specific guidelines drawn up in the IOSS working group of the DG Taxud. These guidelines say that "each order is considered a separate supply irrespective of whether it is a single vendor or underlying supplier selling via electronic interfaces. As each separate order/supply does not exceed EUR 150, the IOSS should be applied by the underlying supplier/electronic interface registered in the IOSS. If multiple orders are packed together they will be considered as single consignment".

Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments? ☒YES, fully implementing the recommendation

Specific indications issued in the 2017 in which, among other things, the selection of operators for PCA involves also who import goods at risk of under-invoicing. In addition, the SIDDA IT procedure carried out a periodic detection of the anomalous values of certain parameters of customs declarations (statistical value/weight; additional statistical value/additional unit [if available]; additional weight/unit [if available]). Based on these findings, the Statistical Analysis Office sent an e-mail to the Registration Offices (Customs/S.O.T.) for each (single) transaction that was found to be outlier for the purposes of ex post controls. Specific guidelines for combating under-invoicing in after-examinations are also included in the guidelines for the controls issued in the 2011. It is also pointed out that - the Italian Government has

CY	Q.**1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?**☒ NO *We are in the process to implement a new system in 2022.* Q**. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?**☒YES, fully implementing the recommendation *Specifications (as rules) were created in the national application to prevent the above cases from being submitted.* **Q. 1.3 Have you ensured that your ECS systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?**☒ YES, partly implementing the recommendation *The risk analysis on low value goods is done manually by customs officers who select for control goods suspected to be undervalued. About 2% of the consignments that are selected for control found to be undervalued.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒YES, partly implementing the recommendation *During manual check of manifest report, customs officers are trying to detect shipments that may concern the same consignment. Such cases have very rarely been identified.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments**? ☒YES, fully implementing the recommendation *A big case of undervaluation was detected concerning the importation of electronic cigarettes from China.* **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?**☒YES, fully implementing the recommendation *Compliance was confirmed.*

LV	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?☒YES, fully implementing the recommendation** *Since 19 November 2019 in Latvia import customs declarations must be lodged for postal consignments. This functionality has been introduced in the national electronic customs data processing system (EMDAS). A strategy of control for postal consignments has been developed and put into practice.Natural persons declare consignments with a value exceeding EUR 22. Import customs declarations for postal consignments are released after the risk analysis has been done. Consignments with value of less than EUR 22 are subject to control measures within the Customs Control Point. Consignments are diverted for control in the event of justified suspicions or random selection. Risk mitigation measures are also implemented for customs declarations with total amount more than 500 (EUR or USD) with a view to preventing unjustified use of the additional procedure C07(consignments of negligible value).* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?**☒YES, fully implementing the recommendation**.** *Electronic customs data processing system does not allow to automatically apply claimed duty relief on postal consignments with a value of more than EUR 150.Risk profile has been created especially to control gifts and goods eligible for relief (additional procedure C08 (consignments sent from one private individual to another), 59S (VAT exemption) and 29S (Customs duty: 2.5% for goods received by individuals in consignments from private persons or travellers' personal luggage)).* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?**☒YES, fully implementing the recommendation**.** *The possible unjustified use of customs tax reliefs for low-value consignments is prevented by risk profiles designed to select consignments of goods to in-depth customs control. For postal consignments one of main risks is undervaluation and specific risk profiles have been set up to tackle this. Risky companies and natural persons are profiled, but taking into consideration the huge amounts of postal consignments main risk mitigation measure is random profiles with specific criteria. Consignments where customs debt is less than EUR 10 may not be charged (not recovered) in accordance with Article 88 of Regulation 2015/2446. It is taken into account in the preparation of risk profiles.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒YES, fully implementing the recommendation *Cases of artificial splitting of consignments are identified in the post-clearance process, by analysing the consignees list and by selecting the consignees with the biggest number of submitted declarations. National Customs board of Latvia is sending the information to authorised authority in the State Revenue Service to carry out audits.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments? ☒YES, fully implementing the recommendation** *Consignees who receive a lot of low-value consignments in short time period are identified for the risk of unregistered business, therefore National Customs board of Latvia is sending this information to authorised authority in the State Revenue Service to carry out audits.* *It is not common practice to carry out post-clearance checks on low-value consignments, since the benefits are disproportionate to the amount of recovered duties. In Latvia, controls for small-value shipments are carried out during customs clearance stage. However, where there is an obvious irregularity and customs debt is more than EUR 10, customs declarations are selected for post-clearance verification.* **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** ☒YES, fully implementing the recommendation *Authorised economic operators (AEOs) are not excluded from checks during customs clearance as well as from post-clearance checks.*

LT

Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?☒YES, partly implementing the recommendation

The Customs of the Republic of Lithuania has developed and approved its Operational Strategy in the Area of Controls that defines the fields, methods, organisational measures and actions of the controls. The control of e-commerce is among the fields of controls defined in this Strategy. To ensure the customs control in the manner prescribed by the law, the Customs of the Republic of Lithuania carries out the all the customs controls by applying various methods and measures that are, in its view, necessary to ensure the right application of the customs operational rules and other legal acts regulating the movement of goods between the customs territory of the Community and the third countries or in the customs territory of the Community. The customs controls are ensured in the following three stages 1) prior to the customs clearance of goods; 2) at the time of the customs clearance of goods; 3) post to the customs clearance and release of goods. The controls of the goods at the time of the customs clearance and after the customs clearance is based on the risk assessment results. The detailed customs valuation control at the time of the customs clearance and after the customs clearance is regulated by the Rules of Controls of the Customs Valuation of Imported Goods approved on 28 April 2004 by Order No. 1B-431 of the General Director of the Customs Department under the Ministry of Finance of the Republic of Lithuania. The above-mentioned Rules indicate the measures applicable to the controls of customs valuation, the items and documents subject to controls and decisions to be taken by the customs official performing the controls.

Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?☒YES, partly implementing the recommendation

1. In accordance with Article 141 (3) and (4) and Article 144 of the Commission delegated Regulation (EU) 2015/2446, postal consignments are declared by providing the forms defined by the Universal Postal Union (CN22, CN23, etc.):

(a) where value of the goods in the postal consignment does not exceed EUR 1 000;

(b) no application for repayment or remission is made in relation these goods;

(c) they are not subject to prohibitions and restrictions.

(AB Lietuvos Pastas is the postal service provider in the Republic of Lithuania. Therefore, AB Lietuvos Pastas alone may carry ou the import, export and transit of postal consignemnts by using CN22, CN23 form declarationas in the Republic of Lithuania).

(d) Postal undertaking sorts the goods received in the postal consigmnments in the distribution centre:

-where value of the goods in the postal consignment is higher than EUR 22 Eur but lower than EUR 150, the customs calculates the VAT on importation;

- where value of the goods in the postal consignment is higher than EUR 150 Eur but lower than EUR 1000, the customs calculates the customs duty, excise and VAT on importation A local risk is applicable and all the goods brought in postal consignments are subject to customs controls by scanning.

Where criteria set out in (a)-(c) are not met or where the senders or receivers of the goods whish to declare the goods themselves (having informed the Lithuanian postal undertaking about that in writing (e-mail, phone) prior to the provision of the goods in postal consignments to the customs, a standard electronic import declaration should be submited on the electronic Customs Clearance Systam (MDAS). Therefore, here an automated risk assessment is applied.

2. Carriage of consignments without using the forms defined by the Universal Postal Union (CN22, CN23, etc.):

(a) low value good (up to EUR 22) carried in small consignments (e. g. by Express courriers) may be subject to oral declaration. In these cases, local risk may be applicable

LU	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?**☒YES, fully implementing the recommendation *In addition to the general electronic customs clearance system (PLDA IETA) and its rules engine applicable for electronic customs declarations, Customs deployed an IT solution (DAkOTA) especially dedicated to electronic risk analysis of structured pre-arrival consignment-level data related to low value shipments. This system is used to perform pre-arrival safety & security, national prohibitions & restrictions and fiscal risk analysis. The data is exchanged on a regular basis with LU competent authority for VAT. Customs controls are based on electronic risk profiles as well as on manual selection by customs officers. This dedicated IT solution for LVC risk analysis was set up in order to best meet the provisions of art. 104 (Waiver to lodge entry summary declarations in regard of LVC < 22 EUR) as well as of art. 141 (Acts deemed to be a customs declaration, LVC < 22 EUR) of Commission delegated regulation (EU) 2015/2446 of 28 July 2015. DAkOTA is primarily used for risk analysis purposes and the data provided there is not to be considered as electronic customs declarations as such. The latter are lodged in PLDA IETA whenever required.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief? ☒YES, fully implementing the recommendation** *Customs implemented both declaration processing and risk rules in their electronic customs clearance system in order to prevent the misuse of relief codes. AEO's are not excluded from these rules. Post-clearance controls by Audit unit also cover declarations declared under LVCR.* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?** ☒YES, fully implementing the recommendation *For this purpose, apply electronic risk profiles as well as random selections. Any available risk information on LVC is assessed and the necessary risk profiles are created whenever relevant.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒YES, fully implementing the recommendation *Making LVC data available by electronic means allows inter alia the alphabetic sorting of operator names, which is efficient in this regard. Furthermore, the detection of this risk is in the scope of post-clearance checks.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☒YES, fully implementing the recommendation *The Audit Inspection regularly monitors LVCR imports. Searches are carried out manually and focus on consignees and as well as on goods. The purpose of the checks is to detect commercial networks and goods' under-valuation.* **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** ☒YES, fully implementing the recommendation *Customs do not distinguish between economic operators.*

HU

Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?☒YES, fully implementing the recommendation

Cross-border e-commerce in particular creates possibilities for the abuse of low-value consignments reliefs, requiring the Customs authorities to take coordinated action to prevent, detect and contain them and ensure traditional own resources are properly recovered. As a rule, the legal frameworks and possibilities in law for action by the Customs authorities are provided for in the Union's customs legislation, which does not recognise e-commerce as a separate concept and does not prescribe separate procedures relating to it. With regard to cross-border e-commerce, the National Tax and Customs Administration (NTCA) drew up a separate strategy for 2020, taking into account the initial recommendation made in the PIF report for 2018. On 1 January 2021, an EU package will enter into force that will fundamentally change how small-value consignments are handled: VAT will have to be paid on them irrespective of the amount involved and, to ensure VAT is recovered, data will have to be submitted in advance. Basically, the centralised operational risk assessment incorporated in the processing of customs procedures serves to eliminate possible abuses. However, the Customs administration receives data only about consignments with a value exceeding EUR 22, which the customs data processor allows to be entered into the system. The risk assessment is therefore automated. Consignments registered as having a value of less than EUR 22 may not be recorded in a customs declaration, so the customs authority does not possess the data on the basis of which those items could have been made subject to centralised operational risk analysis. Low-value consignments delivered via e-commerce are typically, though not always, sent by mail or courier, so the task falls specifically within the remit of the NTCA's Airport Directorate. There is close cooperation between postal and courier services; the scope and tasks of Customs and the postal services are laid down in so-called 'technological agreements'. In 2019, the NTCA's Airport Directorate inspected a total of 929,893 consignments; of these, 87,711 were selected for further inspection following a risk assessment. If the customs inspection concluded that the value of goods in the consignment exceeded EUR 22, the NTCA's Airport Directorate requested documents furnishing proof of the true customs value (the original invoice and proof of payment) from the customs broker. On the basis of the documents provided, more than 80% of the items selected revealed that their respective consignments had arrived undervalued in order to evade customs and VAT payments. However, a declaration of the true customs value is submitted on the basis of the documents enclosed by the customer, so the goods can be released for free circulation only when the customs and VAT payments have been made. It should also be pointed out that, on several occasions in 2019, an inspection revealed other infringements. For example, goods infringing intellectual property rights or products subject to prohibitive or restrictive measures were detected in consignments registered for a duty-free procedure. In the light of the above, it can be said that, both for consignments of less than EUR 22 in value and those of more than EUR 22 in value, the NTCA's Airport Directorate implemented measures in keeping with the objectives of the above strategy by carrying out a centralised operational risk analysis with a full manual handling risk assessment or detection activities inherently linked thereto.

Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief? ☒YES, fully implementing the recommendation

Where the scope of items (e.g. items subject to thresholds or quantitative limits) under Council Regulation (EC) No 1186/2009 setting up a Community system of reliefs from customs duty permitted, filters were incorporated into the customs data processing system (through IT development) and, in certain cases, systematic risk profiles were generated.

Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?☒YES, fully implementing the recommendation

For low-value consignments, more risk profiles have been put in place since the middle of 2019 onwards.

MT	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?**☒NO *The Customs Electronic System does not cater for detection of such declarations however a selection of these declarations are still verified through post clearance checks and through random selection.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief? ☒NO** *A change (upgrade) in the Customs electronic system will be requested from our service provider to address points (a), (b) and (c) of this question.* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?** ☒YES, fully implementing the recommendation **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒NO *By artificial splitting, it is being understood that an individual may order 100 pieces of product 'A' from supplier 'X' and then orders the supplier to ship the goods in 4 different consignments of 25 pieces each so that the value of each consignment will not exceed 150 Euro. The assumption here is that the 4 consignments are delivered under 4 different transport documents with the consignor bearing Supplier 'X' and the consignee bearing the name of the individual who ordered the goods in the first instance. In this instance the Customs system does not have the capabilities to highlight that these four consignments cumulatively form one whole original consignment, the value of which exceeds 150 Euro. In this vein, the Department is eager to learn whether such a detection mechanism exists and how it works so that it can be deployed locally.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments**?☒YES, fully implementing the recommendation **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** ☒YES, fully implementing the recommendation

NL	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?**☒YES, fully implementing the recommendation *E-commerce: We started with a number of e-commerce companies to decrease the risk of low value consignments, this is done in close cooperation with the tax authorities and FIOD. Based on the conclusions of the audit of the European court of Auditors (ECA) regarding VAT and customs duties The Netherlands concluded a number of enforcement activities. Those activities were focusing on the import declarations and post clearance audits.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?**☒NO *We don't have implemented this in our system due to the fact that the customs value is not the same as the intrinsic value of a consignment (insurance costs and freight are not included).* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?**☒YES, fully implementing the recommendation *We have risk profiles.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒YES, fully implementing the recommendation *We have developed and implemented a monitoring tool.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☒YES, partly implementing the recommendation *We have post clearance audits at a number of companies.* **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?**☒YES, fully implementing the recommendation *No different approach.*

AT	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?**☒YES, fully implementing the recommendation *Austria applies a multi layered risk analysis and control approach following the principles "control when required, where required and with the most appropriate control measure". The Austrian risk management approach in the field of low value consignments is a combination of specific electronic risk profiles, risk profiles with a minimum control quota and focal control operations beside the electronic targeting system.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief**?☒YES, fully implementing the recommendation *There are logical routines in the electronic customs systems which check the submitted data to exclude the risks of submitting falsified declarations. Whenever necessary these routines are supported by specific risk profiles.* Q**. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly**?☒YES, fully implementing the recommendation *AT applies specific risk profiles as well as profiles for minimum control quota.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒YES, fully implementing the recommendation **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments? ☒YES,** fully implementing the recommendation *Ex post controls are carried out based on risk analysis. The risk "economic operator" is taken into account in the selection of cases subject to ex-post controls.* **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks**?☒YES, fully implementing the recommendation

PL

1.1 Have you enhanced and enforced your customs control strategies for cross-border e commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?☒YES, partly implementing the recommendation.

In September 2018 the National Revenue Administration (KAS) started work on optimising the clearance and control of e-commerce consignments. The main aim was to assess the amount of duty that might be raised in the event of 100% checks on packages, assuming that each package was a mail order delivery, and the time and money it would cost the Administration to do so. The checks suggested that it would take an official assigned to carry out a 100% check on a consignment 1 working hour to receive and process the documents received from the consignee and to check them against the customs declaration.

In the light of the above actions and Article 144 of Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code, a new customs clearance model was designed for postal traffic. The document proposes new legal, organisational and IT solutions connected with the need to introduce solutions 'sealing' traffic in low-value consignments (e-commerce).

Work is now under way to adapt the customs clearance model for goods in consignments carried by postal and courier services. This is connected with the entry into force on 1 January 2021 of new tax rules, namely the VAT e-commerce package that translates into changes to EU customs rules through amendments to the Union Customs Code Delegated Regulation and the Union Customs Code Implementing Regulation. In the case of postal traffic, the amendments will have a broader reach than the VAT e-commerce package, as they will tie in with changes in Poczta Polska S.A.'s role in customs formalities. This change will see the postal operator making customs declarations as the indirect representative of the consignees of postal consignments. Introducing the changes arising from the new clearance model entails adjustments to the national IT systems handling postal and courier traffic, major organisational changes and amendments to national law, especially tax law and customs rules, in particular the Regulation of the Minister for Finance of 17 August 2016 on customs declarations in postal traffic (Journal of Laws, item 1293).

Owing to the need to introduce 'sealing' solutions for low-value consignments, a national analytical unit (Strategic Analysis Centre) is preparing the terms of reference and scope of operations for checking postal and courier consignments containing low-value goods.

1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?☒ YES, partly implementing the recommendation

Re a) In the system for handling import declarations, for goods with the additional procedure code C07 for customs duty relief for goods up to a value equivalent to EUR 150 (data requirement 1/11 from Annex B to Commission Delegated Regulation (EU) 2015/2446 - equivalent to the second section of box 37 of the SAD) a rule has been introduced triggering the need for the customs authority to check that the value of the consignment does not exceed the equivalent of EUR 150 (duty relief under Article 23 of Regulation (EC) No 1186/2009).

Re b) Goods declared as gifts (duty relief under Article 25 of Regulation (EC) No 1186/2009) are largely declared as postal consignments under Article 141(3) and the second subparagraph of Article 144 of Commission Delegated Regulation (EU) 2015/2446, which means that a customs declaration is submitted in the form of an act deemed to be a customs declaration using documents CN22 and CN23; the electronic customs declaration is not used in such cases.

In other cases, e.g. courier consignments, electronic customs declarations are entered in the system for handling import declarations. However, because consignments of this type also benefit from VAT relief, they are declared in the form of a summary declaration (a number of consignments in a single-item declaration), so automatic checks on whether the value of a single consignment exceeds the ceiling for relief from customs

PT

Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)? SPF Finances (douane) ☒YES, partly implementing the recommendation

Portugal has significantly enhanced its control strategy for combating traditional own resources fraud to cover all electronic customs declarations, and systematically applies risk analysis parameters based on risk indicators/risk profiles. Electronic declarations concerning e-commerce are covered by these measures when processing is mandatory. As regards the other declarations, PT is developing an IT support system for processing electronic declarations relating to low-value consignments, in line with the timetable for COM/MASP-C (the European Commission's Multi-Annual Strategic Plan for Customs). In accordance with our planning, the system will be linked to a risk analysis system in which specific risk profiles will be entered in order to analyse and mitigate the risk associated with low-value consignments traded on electronic platforms (e-commerce consignments).

Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?☒YES, fully implementing the recommendation

The system for automatically processing import customs declarations (STADA - Imports) does not allow the additional scheme code C07 to be declared if the value of the declared goods is in excess of EUR 150, nor does it allow code C08 to be declared if the value of the declared goods is in excess of EUR 45. In order to declare other additional scheme codes in the C series (Relief - Regulation (EC) No 1186/2009), the declarant must make a request to that end, to be analysed by the customs official responsible. STADA - Imports also requires that the TARIC code always be declared in box 33 (Commodity code) of the import declaration in order to ensure that prohibited goods cannot be cleared or that no import restrictions apply to the goods or, if such restrictions apply, that they are complied with.

Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?☒YES, fully implementing the recommendation

LVC declarations that qualify for duty relief pursuant to Article 23 of Regulation (EC) No 1186/2009 are customs cleared (released for free circulation and consumption) by virtue of their being presented to customs. Clearance through presentation to customs is processed using an electronic system that is linked to the risk analysis system (SSA - Sistema de Seleção Automática (Automatic Selection System)). The SSA systematically assesses the risk associated with each LVC. If a risk is identified through the combination of risk indicators based on risk profiles, the SSA selects the relevant consignments, which then undergo a physical check by a customs officer.

Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?☒YES, partly implementing the recommendation

Risk profiles, which combine risk indicators, are applied. Some of these indicators combine the declared value and, for example, the average weight, identifying possible inconsistencies. The systems are set up to detect situations where a split consignment is declared under the same transport document. Measures to enable the potential identification of split consignments carried on different means of transport or under the cover of different transport documents are being examined for implementation. They are based on the analysis of the frequency associated with an operator and other data in the declaration. Such measures are likely to be introduced from next year (2021).

Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments? ☒YES, partly implementing the recommendation

RO	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?** ☒YES, partly implementing the recommendation *-Ministry of Public Finances – National Agency for Fiscal Administration – General Directorate of Customs*: *The fast development of the international e-commerce of goods and the increasing of the volume of low value shipments, as a result of the orders made by using the Internet made the adaptation of the customs authority activity through appropriate measures necessary, in order to facilitate the legitimate trade, to ensure a fast customs clearance process, and at the same time, for managing potential risks related to safety and security. In this respect the General Directorate of Customs was focused on: 1. To improve cooperation with public authorities, national/international organisations and private stakeholders for identification and prevention of the customs and/or fiscal frauds in the field of cross-border e-commerce. For instance, in 2018 the General Directorate of Customs concluded a Protocol with the National Company Posta Romana SA; at the same time, there are also in place protocols concluded between Customs and the most important express courier companies, outlining each other's roles and responsibilities. Those Protocols give a commitment to cooperation between high-level management. Romanian customs authorities have established inter-agency cooperation agreements with relevant government authorities to prevent illicit trade and fraud (e.g.: Romanian Border Police, National Police). 2. To participate to the Joint actions/national operations- i.e.: POSTBOX at European level focused on counterfeiting and drugs. At the same time national customs operations were carried out quarterly, focused on undervaluation of goods- LVCR. 3. To improve risk analysis and management, in order to prevent and fight against infringement of the customs/fiscal legal regulations on cross-border e-commerce. 4. To participate to and carry on training/guidance activities at national and local level. 5. To monitor monthly the results of the customs controls performed on the postal/express couriers consignments as far as the difference between the value declared and the value effectively paid which is to be reflected in the VAT and customs duties (if applicable). At the same time, the type of goods submitted to the customs clearance is already taken into account in order to avoid the impact on the national/EU financial interests (e.g.: intellectual property rights field). It can be highlighted that the Romanian Customs has developed an E-commerce Strategy containing measures meant to improve the customs controls on the postal/express courier consignments. The Draft is under consideration (in order to be approved) at the top management level.For the future the General Directorate of Customs has in view:* • *To continue to participate to the meetings organised under the Customs Against Internet Crime (C@IC) action, within the current 10th Action Plan of the Customs Cooperation Working Party 2020-2021* • *The collaborative work with partners (NC Posta Romana SA and Express couriers) to be strengthened, more focused and developed;* • *Joint actions/operations to be encouraged;* • *Risk analysis and control activities to be enhanced;* • *Training activities at national and local level to be carried on.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?**☒YES, fully implementing the recommendation *Ministry of Public Finances – National Agency for Fiscal Administration – General Directorate of Customs: In 2018 a permanent risk profile was implemented at national level in the IT system that imposed the verification of the customs value declared for all the declarations containing the additional code CO7.* ***Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or***

Sl	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)**?☒YES, fully implementing the recommendation *Financial Administration of the Republic Slovenia answer: Financial administration of the Republic of Slovenia has enhanced and enforced Slovenian customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR) mostly by Slovenian risk analyses system (risk profiles).* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?**☒YES, fully implementing the recommendation *Financial Administration of the Republic Slovenia answer: The Slovenian electronic customs declaration systems does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief. This is ensured by Slovenian risk analyses system by means of risk profiles.* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly**?☒YES, fully implementing the recommendation *Financial Administration of the Republic Slovenia answer:The Slovenian electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles.* *Q***. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?**☒YES, partly implementing the recommendation *Financial Administration of the Republic Slovenia answer: The prevention of artificial splitting of consignments, aiming to benefit from duty relief is ensured by Slovenian risk analyses system by means of risk profiles, and agreement between Slovenian post and Financial administration of the Republic of Slovenia.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☒YES, fully implementing the recommendation *Financial Administration of the Republic Slovenia answer: All the consignments of e-commerce are entered into Import Customs System (ICS) with metadata (such as consignor, consignee, short goods description, the price, the transport fees, customs code – not obligatory), which are available in time of release goods for free circulation. The approach for selection traders ex-post controls in this area takes into account the parcels frequency of imports for particular consignor and/or consignee, the value of goods (low-value), the description/nature of goods.* ***Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?***☒*YES, fully implementing the recommendation* *Financial Administration of the Republic Slovenia answer: In the ex-post controls, the authorised economic operators (AEOs) are not be excluded from such compliance checks. If the AEOs will be hit by the approach mentioned above, the controls will be performed independent of their status.*

SK	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?** ☒YES, fully implementing the recommendation Present process: *Goods are released into the free circulations, on entry of postal consignment - based on the CN22 or CN23 declaration, where the declaration is fully completed and the customs officer considers the data to be relevant. In other cases, when doubts arise as to the relevance of CN22 / CN23 or the data are incomplete, the Slovenská pošta, a.s. (the national post office company) requires from the consignee to prove the value of the goods.* *Slovakia has "Official-duty assessment system", Slovenská pošta, a.s. - the posting department issues and sends to the consignee a "Postal notifications" - information on the arrival of a consignment which is subject of the customs supervision. Via the "Postal notifications", the consignee is notified of what kind of document or evidence must be presented to the customs office for the purposes of the customs clearance. If there is no doubt about the classification of the goods under the Customs Tariff, the customs clearance takes place resulting in the decision to release of the goods to the free circulation, which include the amount of the customs duty. The customs office hands over this decision in case of the representation to the Slovenská pošta, a.s., which delivers it to the consignee together with the consignment. Goods are considered as released for free circulation when delivered to the consignee. The customs debt and other payments are payable upon receipt of the goods in the form of a cash on delivery directly to the post office.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?** ☒YES, fully implementing the recommendation *Customs clearance is done electronically, but not all procedures for postal consignment are fully electronic and automatic, Slovenská pošta, a.s. works on the development of the electronic declaration system related to the e-commerce.* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly?** ☒YES, fully implementing the recommendation *The risk profile warning checks all consignments for which the national mode code C07 (low value shipments up to 150 €) is applied and these consignments, for which the code has been applied illegally, are regularly captured, as the value of the goods on the invoice was higher, or the goods were incorrectly declared.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?** ☒YES, fully implementing the recommendation *Consignments submitted by Slovenská pošta, a.s. are inspected by customs officers daily, by physical checks, by scans, by sniffer dogs and in justified cases also by other control authority which are invited (Slovak Business Inspection, Health and Veterinary Inspections etc.). The risk analysis is based on the generating a risk profile in IT system and the experience of customs officers obtained by daily physical inspection of consignments. For targeting consignments customs officer check consignor's country, repeating consignee, shape and size of consignments etc.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty** Declared consignments of negligible value are also checked when carrying out post-clearance checks. If any irregularities are identified, measures are taken to additionally assess the customs debt. The national post-release control plan for 2020 contains a specific focus on post-release checks on low value shipments. **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** ☒NO

FI	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?** ☒YES, partly implementing the recommendation *Low-value consignment reliefs have been taken into account in the ex-post control planning of the Finnish Customs. The Finnish Customs has a control plan "Undervaluation through e-commerce" which is updated regularly. For example, we analyse the operators in cross-border e-commerce trade. For low-value consignments reliefs we have a risk profile with random sampling (Q. 1.3).For low-value consignment reliefs Finland have had short term operations (one day) concerning courier services. In the control plan, 2020 there will be an audit concerning a courier service. In the end of the year 2020 we will start to use a new risk profile system in import declaration system. The new system has improved features also in tackling the potential abuse of LVCR.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?**☒NO *At this moment, we do not have a risk profile but we are planning to set a risk profile with random sampling.* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly**?☒YES, partly implementing the recommendation *For low-value consignments reliefs we have a risk profile with random sampling.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?** ☒YES, partly implementing the recommendation *The Finnish Customs have included one post-release audit of express courier in to our ex-post control plan 2020. In this audit, the Finnish Customs will examine also the splitting of consignments.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments**? ☒YES, partly implementing the recommendation *In the ex-post control plan 2020 of the Finnish Customs, we have one post-release audit of express courier. In this audit, the Finnish Customs will control the courier´s compliance with the LVCR.* **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** ☒YES, fully implementing the recommendation *Authorised economic operators (AEOs) are included in the control planning of the Finnish Customs. In our ex-post control plan 2020, we have two monitoring audits of AEO express couriers. In these monitoring audits, the Finnish Customs will evaluate the criteria of the AEO status. The AEOs internal control processes and the management of the low value consignments will be evaluated.*

SE	**Q.1.1. Have you enhanced and enforced your customs control strategies for cross-border e-commerce trade, particularly for the potential abuse of low-value consignments reliefs (LVCR)?** ☒*YES, partly implementing the recommendation***.** *The solution used in Sweden means that Swedish Customs is notified for all arriving low value consignments via declaration CN22. Decision for release of goods is sent electronically from Swedish Customs to the designated UPU operator in Sweden. For consignments where VAT is payable additional information is added to the CN22 declaration to enable a correct calculation of the VAT amount. The designated UPU operator ensures that the consumer is willing to pay the VAT amount before clearance of the consignments, if not the consignment is returned to the sender.* **Q. 1.2 Have you ensured that your electronic customs declaration system does not automatically apply claimed duty relief on goods with (a) the declared intrinsic value above EUR 150, (b) on commercial consignments declared as gifts and (c) on goods ineligible for relief?** ☒*YES, partly implementing the recommendation: Low value consignments, procedure C07, with a total value above 2500 SEK is re-routed for post clearance control in the customs clearance system. Consignments with a value below 2500 SEK is automatically cleared. As the 150 EUR only consists of the value of the goods 2500 SEK also includes additional costs which should be added to the customs value. Gifts, procedure C08, is possible to declare with values above 500 SEK on a single item in the declaration. If the value is above 500 SEK the declaration is re-routed for post clearance control in the customs clearance system, similar to the cases regarding C07.* **Q. 1.3 Have you ensured that your electronic customs declaration systems systematically detect potentially undervalued or incorrectly declared goods under LVCR by means of risk profiles or randomly***?* ☒*YES, partly implementing the recommendation. The customs clearance system has a risk profile which randomly selects declarations in the system. This enables the authority to randomly detect goods that might be undervalued. Declarations selected by the random risk profile is then evaluated and might undergo physical inspections.* **Q. 1.4 Have you ensured that there are any specific control measures in place to prevent artificial splitting of consignments, aiming to benefit from duty relief?** ☒*YES, fully implementing the recommendation***.** *Artificial splitting is most common on exit declarations for customs warehousing. To prevent this, the customs clearance system for import does not accept the combination of procedure code 4071 with C07. From 19 February 2019 it is only possible to declare the C07 in combination with the following procedure codes***:** *4000***,** *4200***,** *4500.* **Q. 1.5 Have you ensured that ex-post controls include verifications on traders' compliance with customs duty relief for low-value consignments?** ☒*YES, partly implementing the recommendation***.** *As mentioned in question 1.2 and 1.4 procedure code C07 low value consignments is only accepted in the customs clearance system if combined with procedures 4000, 4200, 4500. Consignments with values above 2500 SEK is re-routed for post clearance control. Swedish Customs is now working to correct declarations where procedure code C07 have been misused and charge the declarant of due duties. Courier companies have been audited during 2019 and these operators have included own system checks to prevent the misuse of C07 in their declarations. During 2020 Swedish Customs aim for the re-routing for post clearance control to be changed to pre-release controls instead. As a general rule customs value is always a topic of Swedish Customs' post clearance controls. This includes control of the low value regulations. However, controls of the low value regulations might have a lower priority in a post clearance control if the risk evaluation shows higher risks elsewhere. Swedish Customs always conducts a risk valuation to pin point where the highest risks are in the control* **Q. 1.5.a. Are authorised economic operators (AEOs) not excluded from such compliance checks?** ☒*YES, fully implementing the recommendation. Sweden does not exclude AEOs from any analysis or risk profiles.*

2.2. EXPENDITURE

BE	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?** AFCOS BE (ICCF)☒NO *The national anti-fraud strategy is currently being prepared, in collaboration with the federated entities that manage European funds and customs. It should be adopted at the end of 2020.* **Q.2.2.a In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?** ☒YES, partly implementing the recommendation *ERDF Wallonia: The Management Authority of the Wallonia 2020.EU (ERDF) programme still uses the ARACHNE tool.* *ERDF Brussels-Capital Region: The ERDF Management Authority of the Brussels-Capital Region has boosted its control of the result indicators provided by the coordinators of financed projects, by implementing a new generalised and systematic control procedure.* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?** ☒YES (ERDF Wallonia) ☒NO (ERDF Brussels-Capital Region). *ERDF Wallonia: Signing by the beneficiaries of a declaration of absence of conflict of interests in public procurement contracts, Continued use of the ARACHNE tool* *ERDF Brussels-Capital Region: We do not have complete documents listing those results.* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?** ☒YES, partly implementing the recommendation *ERDF Brussels-Capital Region: The fraud detection measures have been set up within the Management Authority of the ERDF Brussels-Capital Region, both in terms of analysis of public procurement and conflict of interest. For 2020, the Management Authority is considering carrying out an extensive control concerning compliance by project coordinators with State aid legislation.* **Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?**☒YES, partly implementing the recommendation *ERDF Wallonia: The Management Authority has procedures in place for reporting fraud cases both internally and to the European Anti-Fraud Office. All reported cases are treated in the strictest confidentiality and in accordance with personal data protection legislation. Furthermore, in its regional policy declaration (2019-2024), the Walloon Government has committed to recognising whistle-blower status by ensuring the protection of any official who, in good faith, reports criminal behaviour within*

	his/her administration, and to extending application of this status across regional and local public services, in line with what has been adopted at the federal administration level. This process is therefore ongoing. *ERDF Brussels-Capital Region: The Management Authority of the ERDF Brussels-Capital Region has not set up a specific system enabling spontaneous reporting of irregularities and/or fraud. However, in the event of any such reporting by means of, for instance, sending an e-mail directly to the service, the Management Authority carries out an in-depth audit of the project on the basis of the behaviour reported and carries out, where applicable, any resulting financial corrections. Over the course of the current programming, only one such report has been made to the Management Authority. It concerned the submitting of incorrect time-sheets intended to substantiate unjustified work time that had not been spent on the project.* **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?**☒YES, partly implementing the recommendation (ERDF Wallonia)☒NO (ERDF Brussels-Capital) *ERDF Wallonia: Management Authority staff are bound by Article 29 of the Code of Criminal Procedure to report immediately any fraud or suspicion of fraud to the competent Public Prosecutor.*

BG	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF**?☒ YES, fully implementing the recommendation *In summary record No 53 of the meeting of the Council of Ministers of 17 December 2014, Bulgaria adopted a national strategy for preventing and combating irregularities and fraud affecting the financial interests of the European Union for the period 2014-2020. The European Commission was officially notified of this fact. The AFCOS Directorate of the Ministry of Interior also sent the strategy in Bulgarian and English to the European Anti-Fraud Office (OLAF) in 2015 and uploaded it to the CIRCA BC information sharing platform for working groups. In 2019 Bulgaria launched the process of drafting a national strategy for the period 2021-2027 under the management of the AFCOS Directorate of the Ministry of the Interior.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?**☒ YES, fully implementing the recommendation *A national strategy for preventing and combating irregularities and fraud affecting the financial interests of the European Union for the period 2014-2020 was drawn up with the cooperation of all bodies involved in the management and control of EU funds, including the Public Prosecutor's Office of the Republic of Bulgaria. The draft strategy will be endorsed by the Council for coordinating the fight against infringements affecting the financial interests of the European Union (AFCOS Council) established at high political level and submitted to the Council of Ministers for adoption. In 2020 all the national authorities involved in the management and control of EU funds will continue working actively on the draft national strategy for the period 2021-2027.* **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?**☒ YES, fully implementing the recommendation *The national strategy for preventing and combating irregularities and fraud affecting the financial interests of the European Union for the period 2014-2020 takes account of all European Union strategic and regulatory documents predating its adoption in 2014, including the PIF reports. The recommendations of the PIF reports for 2016, 2017 and 2018 are reflected in the annual implementation plan accompanying the 2014-2020 national strategy and in the new national anti fraud strategy being drafted for the period 2021-2027. The new national anti-fraud strategy for the period 2021-2027 will be based in particular on risk analysis and will include a complementary objective: implementation of the recommendations of the European Commission and the European Court of Auditors, including the recommendations of Article 325 TFEU reports.* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;**☒YES, fully implementing the recommendation**.** *The need for coherence between administrative and criminal inspections and investigations is enshrined in the annual implementation plan of the 2014-2020 national strategy. It provides for different activities in this regard, e.g. regular meetings*

between officers of the General Directorate for Combating Organised Crime (GDBOP) (criminal investigations) and the AFCOS Directorate (administrative investigations), round-tables between specialised bodies, etc. Other activities in the annual plan include: improving the interaction between the General Directorate for Combating Organised Crime, the AFCOS Directorate, the Prosecutor's Office, the Customs Agency and the National Security Agency (SANS); the provision by the AFCOS Directorate of information on operational interaction with OLAF, etc. to the National Police General Directorate and/or the General Directorate for Combating Organised Crime. Frequent use is made of joint investigation teams, thereby strengthening ties between the administrative and criminal authorities.

Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?☒ NO

As the National Strategy applies until 31 December 2020, its implementation will be evaluated in the second half of 2020.

Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?☒YES, fully implementing the recommendation

The managing authorities of operational programmes financed by EU structural funds regulate access to ARACHNE through administrative orders specifying the names and positions of those with access to ARACHNE. A significant number of managing authorities' staff have access to ARACHNE: while a small proportion are managers or observers, most are case-handlers.

The use of ARACHNE is set out in the following chapters of the manuals of the managing authorities for individual programmes:

- *in the chapter on risk management and the related risk control*

In order to monitor and prevent the risk of fraud at a managing authority, checks are carried out in the ARACHNE system. There are also procedures for reporting irregularities based on checks in the ARACHNE system.

- *in the chapter on monitoring projects and verifying expenditure*

ARACHNE is used when selecting a sample for on-the-spot checks, when checking State aid in the course of the implementation of grant agreements and when checking and verifying technical reports, payment requests and financial statements accompanying the package of accounting documents. If, when checking a given risk category of beneficiary in ARACHNE, the case-handlers responsible for technical and financial verification find high risk values for a given category of beneficiary, which are highlighted in yellow or red, they check the relevant documentation and information available in UMIS 2020, all public registers and in managing authority databases. Checks are documented by a specific check in the checklists concerned. When checks are carried out, high-risk projects are flagged up to the staff dealing with irregularities so they can exercise particular care when handling the related documents or, if necessary, take appropriate measures.

- *in the chapter on financial management*

Before making any payment to a beneficiary, a member of the accounting unit checks ARACHNE to make sure that the beneficiary does not present a high risk of bankruptcy and/or insolvency and that it is not blacklisted. Where there is a high risk of the above circumstances, the member of staff carries out additional checks within the unit's remit and may request additional information from other departments of the managing authority. If there is reason to suspect an irregularity, the member of staff reports the matter to the irregularities officer in accordance with the relevant chapter of the managing authority's manual.

- *in the chapter describing the steps for providing grants*

The use of the instrument is prescribed in the process whereby members of the committee evaluating and ranking project proposals for the purposes of awarding grants are screened for conflicts of interest before the committee's appointment; the persons appointed to rule on the merits of any objections received are screened for conflicts of interest; screening for conflicts of interest prior to the conclusion of an agreement in project selection/direct award procedures, which requires the use of ARACHNE to assess the risk involved in these processes and rules for verifying and following up cases reported by ARACHNE.

- *in the chapter on irregularities*

The rules and procedures for reporting an irregularity based on a check in ARACHNE are set out.

Continuous training courses on the use of ARACHNE figure in the annual training plans for managing authority staff.

The managing authorities of operational programmes financed by EU Structural Funds can access and use both the official public electronic systems, such as the Commercial Register, containing information on beneficiaries and the electronic systems of the National Revenue Agency (NAP), Sofia Municipality, the Ministry of Justice, the General Labour Inspectorate Executive Agency (GIT EA) and the National Labour Market Database of the Employment Agency. Active use is also made of information from the Management and Monitoring System for EU Funds in Bulgaria (UMIS) 2020.

With regard to the Agricultural Funds, the State Fund for Agriculture, for the purposes of analysing the risk involved in its operations and as part of its battery of instruments, carries out, in the course of its annual planning exercise and in the framework of various audit engagements, risk assessment and analysis on the basis of predefined criteria, including the assessment of quality, good practices, use of IT tools and Arbutus specialised data-analysis software, and the capabilities of the control environment and control activities in place, for the purpose of detecting and preventing situations linked to the occurrence of irregularities and fraud.

The Audit Authority (Executive Agency for the Audit of EU Funds) prioritises the use of the statistical approach when selecting samples for operations audits. All auditors have an ARACHNE user account. ARACHNE is used when planning system audits and, after samples have been selected for each operational programme, when carrying out checks to identify the presence or absence of indicators of irregularities and fraud.

Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?☒ YES

Each year the managing authorities of operational programmes financed from EU Structural Funds take note of the reports' recommendations in the fraud risk assessment process. The process of preparing fraud risk assessments and managing authorities' action plans involves not only prevention and proactive measures to detect fraud following checks by irregularities staff on reports received but also cooperation with prosecutions services, courts and investigating authorities. Examples of cooperation include the checks carried out on suspicions of fraud, the sending of files to the prosecutor's office and the initiation of pre-trial proceedings. ARACHNE is actively used when assessing the risk of fraud, implementing the measures identified and checking reports. Some managing authorities set up fraud risk self-assessment teams comprising representatives of the directorates responsible for project selection and contracting, verification, accounting and payments, risk management and control and representatives of technical assistance teams. The internal operating rules for these teams lay down procedures for monitoring the effectiveness of fraud prevention and detection measures. As regards the agricultural funds, the State Fund for Agriculture carries out intensive coordination activities with other state institutions and law-enforcement bodies with a view to providing the information and documents needed by Bulgaria's investigating authorities and judiciary. These activities are necessary to detect and prevent irregularities and fraud.

In 2019 the Ministry of the Interior's AFCOS Directorate carried out administrative checks on the reporting and management of reports of fraud and irregularities at the State Fund for Agriculture. The inspections were concluded by reports in which, following analysis of the problem areas identified, the AFCOS Directorate made recommendations aimed at making the fight against irregularities and fraud affecting the EU's financial interests more effective. For its part, the State Fund for Agriculture has taken the steps necessary to implement the recommendations made by the AFCOS Directorate.

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?☒ YES, fully implementing the recommendation

When carrying out risk analysis, the managing authorities of operational programmes financed by EU Structural Funds use an approach consistent with the different types of operations, taking into account whether the operation involves project selection or direct award and the amount of the grant and whether the operation is to be carried out using a simplified procedure. In the case of partial implementation, the value of verified expenditure is reduced; if the case involves a failure to meet the set of indicators, a financial correction is made. As regards agricultural funds, every directorate of the State Fund for Agriculture administering schemes and measures co-financed by European Union funds and the national budget has introduced additional controls in the form of lists of fraud indicators (red flags). These red flags determine the scope for additional checks during the administrative handling of projects and applications for support and serve to filter risky applicants out of a procedure. Case-handlers processing candidates' documents are required to carry out further analysis when they encounter red flags. This further analysis helps the entire State Fund for Agriculture take key decisions when an irregularity is found and to take appropriate follow-up by imposing a penalty, investigating suspicions of fraud or recovering grants.

In this context, the Fraud Prevention Directorate conducted two training sessions in 2019, one of the topics addressed being the introduction and use of the lists of red flags. 266 Fund employees underwent such training. The lists of red flags are helping to upgrade and improve the risk assessment and management

system, reinforcing internal controls and increasing the effectiveness of action to detect and counter irregularities and fraud affecting the financial interests of the EU.

From 1 to 3 July 2019, eight officials from the State Fund for Agriculture and one from the Ministry of the Interior's AFCOS Directorate underwent training in countering irregularities and fraud at Croatia's Agriculture, Fisheries and Rural Development Agency. This training continued the good working relationship developed by Bulgaria's State Fund for Agriculture and its Croatian counterpart in countering fraud involving agricultural funds. The purpose of the visit was to share best practices from the measures developed and implemented by Croatia and Bulgaria to combat fraud and irregularities in the management of EU agricultural funds. Risk analysis is an integral part of the Audit Authority's audit work at all levels. Risk assessment is carried out when drawing up the audit strategies for each operational programme, in accordance with Article 127(4) of Regulation (EU) No 1303/2013 of the European Parliament and of the Council, and when preparing the annual audit plan, the annual control report and the schedule of audit engagements. For the purpose of the strategic planning and prioritisation of audit work on system audits, audits of operations and audits of operational programmes, the Audit Authority performs a comprehensive risk assessment covering the management and control systems of the programme concerned (the managing authority and the certifying authority). When selecting the risk-assessment approach, account is taken of the Guidance for Member States on Audit Strategy, the Guidance for the Commission and Member States on a common methodology for the assessment of management and control systems in the Member States (EGESIF 14-0010 of 18/12/2014) and the European Commission's Guidance on fraud risk assessment and effective and proportionate anti-fraud measures.

Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism? ☒ YES, fully implementing the recommendation

The managing authorities of operational programmes financed by EU Structural Funds maintain an 'Irregularities' button on their websites that anyone is entitled to use to report an irregularity, suspected fraud or fraud in relation to the implementation of projects financed by EU Structural Funds. Reports may also be submitted anonymously. Reports may also be submitted by mail to a managing authority's postal address, which is publicly available, by hand at a managing authority's head office or by e-mail. Reports are verified by an irregularities officer, who then informs the whistleblower of the outcome of the verification. By special order, the heads of the managing authorities of operational programmes financed by EU Structural Funds have approved internal rules for the protection of whistleblowers reporting corruption, acts of corruption and/or conflicts of interest at the managing authority of the programme concerned. All irregularity reports are followed up by administrative checks; if necessary, internal and external reports are followed up by unannounced on-the-spot checks. For example, in 2019 two reports concerning suspected fraud under one of the operational programmes by the beneficiary of two different projects led to a total of seven on-the-spot checks by the managing authority's irregularities officers: one on the beneficiary, four on its partners in the two projects, and, following a second report concerning one of the projects, two simultaneous on the-spot checks on the equipment supplied and the two partners. The files relating to the checks carried out under the two reports were sent to the Public Prosecutor's Office for follow-up. The managing authorities of operational programmes financed by EU Structural Funds have laid down anti-fraud policies for their respective programmes, including a policy to combat conflicts of

interest, in line with the European Commission's Guidance for Member States and bodies managing programmes on fraud risk assessment and effective and proportionate anti-fraud measures. Managing authorities' general anti-fraud policies include a strategy for the development of an anti-fraud culture, the allocation of responsibilities in anti-fraud actions, mechanisms for reporting suspected fraud and mechanisms for cooperating with the competent authorities. These policies are approved by the head of the relevant managing authority and published on the managing authority's website. The policy is also usually included in the manual for the management of the programme concerned. As regards the agricultural funds and the fisheries fund, reporting channels at the State Fund for Agriculture are clear within the organisation and guarantee confidentiality.

At the State Fund for Agriculture, reports on fraud and corrupt practices can be submitted:

- *by email toSIGNALI@DFZ.BG;*
- *by telephoning the hotline 0700-106-16;*
- *by submitting, in the case of an outside source, a written report to the Fund's secretariat;*
- *orally, where information is received by a member of the Fund's staff over the telephone; during on-the-spot checks; in person during an open day;*
- *by a member of the Fund's staff.*

Any information received by the State Fund for Agriculture, including from anonymous sources, is written up in a document containing data concerning the alleged or established act/omission by the economic operator concerned. The State Fund for Agriculture has an internal procedure for registering and examining the reports received, complying with the principle of protecting whistle-blowers, and for following up the reports received.

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?☒YES, fully implementing the recommendation

After carrying out thorough checks on reports of irregularities, all managing authorities of operational programmes financed by EU Structural Funds report cases of suspected fraud to the Public Prosecutor's Office. In 2019 three instances of suspected fraud were reported to the Public Prosecutor's Office under only one of the operational programmes. The prosecutions service has followed up all three reports and pre-trial investigations are currently under way. Most cases of irregularities are detected prior to payment, but where fraud is found to have resulted in the payment of irregular expenditure, managing authorities of operational programmes take measures to recover public funds from the dishonest beneficiaries. Managing authorities of operational programmes financed by EU Structural Funds carry out annual training sessions with representatives of the judiciary, at which specific case studies are examined and proposals are drawn up for improving the regulatory framework. In the area of the administrative investigation of suspected irregularities and fraud, managing authorities maintain active contacts with the Ministry of the Interior's AFCOS Directorate. Where necessary, joint on-the-spot checks are carried out, including the participation of officers from the Economic Police Department. As regards the agricultural funds, the State Fund for Agriculture works closely with representatives of the Ministry of the Interior's AFCOS Directorate, the Ministry of Interior's specialised investigative bodies, the managing authorities of operational programmes financed by EU Structural Funds and the Public Prosecutor's Office. Where necessary, the State Fund for Agriculture and the national authorities referred to above hold joint workshops in a variety of formats to discuss matters of relevance to specific cases or to overall policy for preventing and combating

	irregularities and fraud affecting the financial interests of the European Union. The Audit Authority sent 14 final audit reports containing suspicions of fraud identified during the audit checks to the Public Prosecutor's Office for appropriate follow-up.

CZ	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒YES, fully implementing the recommendation *The National Strategy was approved in Government Resolution No 535 dated 14 May 2008. The first amendment of the document, reflecting the legislation development in the EU and in the Czech Republic, came into force on 1 September 2017. In February 2020, an approval procedure for the second amendment has been launched. The second amendment reflects the developments in relevant legal acts as well as the recommendations of the ECA Special Report 6/2019.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?** ☒YES, fully implementing the recommendation *The National Strategy and both of its amendments have been consulted with all relevant bodies and authorities.* *Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports*? ☒YES, partly implementing the recommendation *In order the further improve the effectiveness of the cooperation in detection and prosecution of irregularities in the area of EU financial interests' protection and define the necessary framework for the cooperation in reporting of irregularities concerning specific EU funds, agreements on the provision of information and cooperation were signed between the Central Contact Point (CCP) of AFCOS and the relevant ministries.* *Twice a year, trainings are provided by the CCP of AFCOS to local contact points of AFCOS of the relevant ministries in order to keep them up-to-date with latest developments in the area of protection of EU financial interests.* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;**☒YES, partly implementing the recommendation *As a follow-up to the Action Plan to the National Strategy, agreements on exchange of information and mutual cooperation are being negotiated between the CCP of AFCOS and the Supreme Public Prosecutor's Office as well as between the CCP AFCOS and the Police of the Czech Republic. These agreements shall formalise and streamline the cooperation between those bodies in the area of protection of EU's financial interests.* **Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?** ☒NO

Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?☒YES, fully implementing the recommendation

At the level of Operational Programme, a risk management system is set up, which consists of systematic identification, evaluation, management and reporting of all significant risks, within which due attention is paid to the identification and management of fraud risk. The risk management system is based on the ESI Funds Risk Management Guideline for the 2014-2020 programming period. The Managing Authority's (MA) self-assessment tool is used to carry out regular evaluation of the effectiveness of control mechanisms, which is based on the Methodological Guideline for the performance of controls under the responsibility of MAs in the implementation of the ESIF for 2014-2020. The tool primarily addresses the risks of fraud.

During the administrative verification and on-site control the fraud indicators, described in the Operational Manual, are verified. Relevant chapters of the Manual describe in detail the procedure of the MA staff for identifying and monitoring the possible risk of fraud, including subsequent evaluation, which results in the examination of information in the form of an on-site inspection or the filing of a criminal complaint. The MA has established the Register of Fraud Indicators and the Register of Complaints from Information Systems. Data from both records are entered through the set of risk factors into the interim risk analysis on projects. The interim risk analysis on the projects from which the control plans are generated is carried out on the basis of risk factors (e.g. risk factor Presence on the list of the 10 most risky projects in Arachne, Presence of the applicant on the list of risk entities and the state of affairs, Increased risk of fraud). Information on detected fraud indicators is shared across the MA's departments, which leads to general awareness and gaining experience of individual employees with fraud indicators and their search. All employees have "read" access to both records, so they can continuously get to know the identified cases and the status of their solution. Each department informs its staff about new cases and thereby enhances the quality of performance of further inspections for the same / similar type of projects. In addition, meetings with the heads of administration departments take place twice a year, in which all cases of identified fraud indicators that occurred are presented in an anonymous form, and possible measures are discussed. To this end, the "Theoretical Examples of Fraud" record has been created, with descriptions of the fraud scheme and warning signs. Furthermore, in the MA self-assessment process, all representatives of departments at the level of directors are acquainted with all cases of detected fraud indicators during the reporting period. At present, data mining from Arachne as part of administrative check is being tested. Testing started in April 2019. Data mining is based on the analysis of projects generated as the most risky. Data collection from Arachne is based on the selection of the most risky projects based on the set criteria, where the reasons for the occurrence of increased values of individual risk indicators are being verified. In the event of an increase in values for any of the risk categories, the causes of the increase will be verified as part of the administrative check. The reasons and outcome of the verification are entered in the records that the MA intends to use subsequently when creating the on-site inspection plan.

Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?☒YES

For example in the checklists for on-the-spot checks the MA has added questions about ARACHNE concerning public procurements and contracts or concerning eligibility and efficiency of expenditures. In 2019, the MA's self-assessment and the regular evaluation of the implementation of measures of the Strategy for Combating Fraud and Corruption within the drawing of funds of the Common Strategic Framework in 2014-2020 were carried out. The internal anti-corruption programme for 2018-2020 was updated in 2018. In the case of suspicion of committing a criminal offence (e.g. fraud) and if criminal proceedings have already been commenced in the given case pursuant to Section 158 (3) of Act No. 141/1961 Coll., Criminal Procedure Code, the officers of the control and audit unit of EU funds report these cases as an irregularity through MS2014 + (IRQ3). This procedure ensures the awareness of other relevant authorities such as Payment and Certification Authority, Audit Authority and others. Irregularities over 10 000 EUR of the ESI Funds are secured through OLAF - IMS. The cooperation with the Police of the Czech Republic in the case of fraud has been gradually intensified by written, electronic or phone communication. A special department was created for communication with the Czech Police. The officers of the control and audit unit of EU funds in cooperation with the Intermediate Body provide them with the requested information on specific projects. The ARACHNE information system is used by the Intermediate body, especially before the Grant Decision is issued. Furthermore, the ARACHNE system is also used in other project control activities.

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure? ☒YES, fully implementing the recommendation

During the entire process of programme administration and implementation, the MA monitors the occurrence of fraud indicators:
1) Review in the process of project approval / before the legal act on awarding of the grant
In addition to monitoring the occurrence of the fraud indicator, the MA checks the risk of the applicant / project partner in terms of collision with the list of criminal complaints resulting from the implementation of the projects or its interconnection through ownership structure with other entities or persons that appear on this list. If an increased project risk is identified, it will be taken into account in the risk analysis of the projects.
2) Control in the project implementation process
In the administration of monitoring reports, the occurrence of fraud indicators is assessed in accordance with the relevant provisions. Data from information systems are used to identify risk operations. These information systems include e.g. Arachne, Justice.cz portal, ARES applications, commercial register, trade register and other publicly available information records and registers. Based on discussions on setting risk factors for projects running in 2018, on 1 January 2019, the risk analyses were divided into risk analysis for individual projects and risk analysis for simplified projects, which are in some respects specific and the originally set of risk scale factors were not adequate. In addition, the Annex with risk factors for separate risk analysis for the period of project sustainability entered into force. In the course of the year, the risk factor for individual and simplified projects was supplemented by the risk factor of double financing risk. Based on the experience of the MA with the implementation of procedures for assessing the occurrence of fraud indicators, the risk factor of Increased fraud risk was added to both lists. The MA is obliged to use such identified and evaluated data for its control activities (on-site inspections). This is done in the form of

ad hoc on-site inspections on the basis of a complaint arising from administrative verification or, as the case may be, an external complaint, of which the MA becomes aware. If the MA suspects, on the basis of its inspection activities, that a crime has been committed, it sends a criminal complaint to the Public Prosecutor's Office.

Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?☒YES, partly implementing the recommendation

There is no special legal act for the protection of whistleblowers in the Czech Republic yet, however, such act is currently under preparation (in line with the Directive (EU) 2019/1937). The protection of whistleblowers is solved within the Civil Service Act. Based on this Act each resort has its own Methodological Guidelines, which solve the protection of whistleblowers, reporting of corruption and fraud. In general, there are special websites, e-mail addresses and /or phone lines at each ministry for whistleblowers. Complaints from third parties relating to the implementation of projects from the ESIF are recorded and investigated and dealt with as suspected irregularities. Depending on the nature of the complaint, it is settled whether it will be verified by an administrative or on-site inspection or a criminal complaint may be filed. Based on the outcome of the verification, it is then resolved as a (un)confirmed irregularity or suspected crime. The presentation at seminars for beneficiaries includes information on how to proceed in case of detected corruption or fraud and where the necessary information can be found, including a link to OLAF's website where fraud can be reported. An example of findings detected during on-the-spot check that have been performed because of information received from informants is an irregularity concerning childcare facilities.

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?☒YES, fully implementing the recommendation

Cooperation between individual administrative and judicial authorities and individual procedures are regulated within the relevant chapters of the Operational Manual. The MA continuously communicates with individual financial administration authorities in order to resolve reported irregularities and to clarify different opinions on the cases. Reporting of irregularities and the actual process, including the transmission of information, is also continuously consulted with the Paying and Certifying Authority, Audit Authority and CCP of AFCOS and at the working level within the Working Group on Control, Audit and Irregularities. Reporting of irregularities is carried out in the MS2014+ system, where irregularities of more than EUR 10,000 in EU share are transmitted to AFCOS LCP and subsequently to IMS, accessible to state prosecutors, to give them a quick overview of the case concerning suspected criminal offences. The suspicion of a criminal offence itself is reported to the Paying and Certifying Authority, through the newly established Serious Findings Module to the Ministry of Finance and the relevant Public Prosecutor's Office is also informed. In case of any need, the MA shall ensure cooperation throughout the investigation. A new element in the interconnected system is the SharePoint of the AFCOS CCP, which is to ensure an overview of all judgments concerning damage to the EU's financial interests and, by sharing it with all managing authorities, to ensure concurrence in the execution of the sentence. If, in the case of a public procurement inspection, a suspicion of a misdemeanour is found under the Public Procurement Act, a complaint is sent to the Office for the Protection of Competition.

DK	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒NO *Denmark does not have a national anti-fraud strategy.* 2. Risk Analysis Q**.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?**☒YES, partly implementing the recommendation *The Danish Business Authority: The Managing Authority carries out data analysis, including cross-analysis and risk-based sampling in each reporting period for all projects. In autumn 2014 the Managing Authority tried out a preliminary test of the European Commission's ARACHNE tool, but it has some reservations about compliance with the data protection regulations when using the tool.* *The Danish Agricultural Agency: Has enlisted the help of external consultants from Deloitte to amplify and structure its risk profile for project support (NON-AIACS). We can conclude that switching to standard costs for the rural development programme eliminates some risks, such as manipulation of the tender procedure, but we also need to be alert, from the outset, to any new risks that may result from the model. As regards ARACHNE, the Danish Agricultural Agency is continuously monitoring and evaluating other authorities' and Member States' experiences with the tool.* *The Danish Fisheries Agency: The Danish Fisheries Agency has not implemented the ARACHNE tool, but has focused on strengthening the case handlings procedures. We are currently working on updating our IT system, which will help eliminate attempts to commit fraud.* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?**☒NO *The Danish Business Authority: No examples of fraud were found using OBS lists (data analysis of all reported data). Many examples of input errors or similar errors were found.* *The Danish Agricultural Agency: The Agency uses the PIF reports as input for its risk assessments. Many sources are used for this process and it is difficult to link the results directly to any single source.* *The Danish Fisheries Agency: The Danish Fisheries Agency has reviewed our administrative fundament and case management with focus on the case-handlings-procedures in order to detect fraud or attempts on fraud. Since the new case handling procedures have been implemented we haven't detected new examples of fraud.* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?** ☒YES, partly implementing the recommendation *The Danish Business Authority: Use of OBS lists. There is and probably always will be potential for*

smarter use of data - particularly where there is a very large and growing volume of data.

The Danish Agricultural Agency has carried out a risk analysis of project support, divided into market organisations, schemes with standard costs and schemes with two tenders. The aim was to identify and rank risks in relation to the Agency's current fraud prevention frameworks.

The Danish Fisheries Agency: During 2018 and 2019 the Danish Fisheries Agency has reviewed our administrative fundament and case management. This has led to the detection of cases suspicious of fraud. The areas with the highest risk of fraud have been: stating the correct level of expenditures and maintaining eligibility after completing an operation. These findings have led to updates and alterations in the legislation and our case handling procedures. The measures taken have been risk based, however not on basis of ARACHNE, but national IT tools and especially case handling-procedures.

3. Horizontal issues

Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?☒YES, partly implementing the recommendation

The Danish Business Authority: The Danish Business Authority, MA for ERDF and ESF have specified further guidance for informers of irregularities in the anti-fraud policy.

Last year we launched a new whistleblower scheme, which is based on a web form solution where its possible to anonymously report suspected fraud.

Since 2014 the Danish Agricultural Agency has made it easier for whistleblowers to make contact via the Agency's website.

Since 2014 there has been a portal on the website of the Danish Fisheries Agency where external parties or whistleblowers can report fraud or irregularities. The Fisheries Agency has also set up an anti-fraud mail box to which the public can send reports of suspected fraud involving EU funds.

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?☒NO

DE	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?** ☒*NO* **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?** ☒YES, fully implementing the recommendation *The procedures for risk analysis contained in, inter alia, the fraud prevention manuals of the competent authorities in the agricultural and fisheries sectors shall be continuously adapted to the specific circumstances. Computer systems are also used for this purpose, according to the scope and specification of the risk analyses to be carried out. ARACHNE is not used in Germany. The results of the risk analyses are documented and evaluated by the implementing authorities (paying agencies/managing authorities).* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?** ☒*YES See the reply for Q.2.2.a* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?** ☒*YES, fully implementing the recommendation See the reply for Q.2.2.a* **Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?** ☒NO *To date, there is no comprehensive legal provision in Germany to protect persons providing information. Following the entry into force of Directive (EU) 2019/1937, there is a need for transposition for both the private and public sectors. The Federal Government is working on the necessary measures to ensure that the Directive is implemented by the 16th deadline. December 2021.* **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?** ☒*YES, partly implementing the recommendation*

EE	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒NO Q**.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?**☒YES, partly implementing the recommendation *Regular meetings with different related bodies (The Environment Agency, Competition Authority, other investigative bodies) to discuss the risky projects / support measures to prevent fraud and other problems.* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?**☒YES *Improved risk analyses in order to find cumulative supports to the same land cadasters despite different applicants. The goal is to find artificially created applicants (Rural development measure schemes)* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?** ☒YES, partly implementing the recommendation *We improved risk analyses in order to find cumulative supports to the same land cadastres despite different applicants. The goal is to find artificially created applicants (Rural development measure schemes) + Training courses to raise fraud awareness of the Estonian Auditors' Association and law makers in the Ministry of Rural Affairs.* **Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?** YES, partly implementing the recommendation *In 2019 a draft bill was presented to the Parliament, which amongst other amendments also strengthens the protection of people who report breaches of anti-money laundering measures.* **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?**☐YES, partly implementing the recommendation *Regular meetings with different related bodies (The Environment Agency, Competition Authority, other investigative bodies) to discuss the risky projects / support measures to prevent fraud and other problems.*

IE	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒NO **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?**☒YES, partly implementing the recommendation *Further steps were taken in 2019 by the ERDF Managing Authorities to implement ARACHNE. This included the first batch imports of live ERDF data from the Irish eCohesion system to ARACHNE and training for the ERDF Managing Authority and Certifying Authority staff. This was provided by the Commission's ARACHNE team in May 2019 and led to further development work by the Managing Authorities to align eCohesion reports with the ARACHNE system requirements. The ERDF Managing Authorities also utilise the Irregularities Management System (IMS) for the reporting of irregularities/fraud under the Regional Operational Programmes.* Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?☒NO **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?** ☒YES, partly implementing the recommendation *The ERDF Managing Authorities agreed on an approach to carry out a Risk Assessment on each Intermediate Body submitting a declaration of expenditure to the Managing Authorities. The first set of risk assessments was carried out over the period mid-2017 to early 2018 and utilised the self-assessment checklist provided by the Commission. As these run bi-annually, the Managing Authorities are now in the process of reviewing these with the Intermediate Bodies concerned and are also undertaking Risk Analysis on those Intermediate Bodies that are progressing expenditure to Declaration stage. Both Managing Authorities are represented on a Risk Assessment team that reviews the documentation provided by Intermediate Bodies and will liaise with the national AFCOS representative with a view to its inclusion in the process.* Q**.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism**?☒YES, partly implementing the recommendation *The Protected Disclosures Act 2014 provides robust statutory protections from retaliation for workers who speak up about wrongdoing in the workplace. The definition of "wrongdoing" in the Act is broad and includes, inter alia, any criminal offence (including fraud), failure to comply with a legal obligation and any unlawful or otherwise improper use of public funds (including EU funds) or the resources of a public body. All public bodies are required by law to have formal channels and procedures for receiving and handling reports of wrongdoing from whistleblowers. The statutory guidance for public bodies, which sets out the recommended practice for establishing and operating these channels and procedures provides, inter alia, that, "The control functions of the public body (such as Internal Audit or Compliance) should monitor the operation of the Procedures on an ongoing basis and report to the Audit Committee or equivalent on their finding". The EU Whistleblowing Directive, which entered into force on 26 November and must be*

	transposed by 17 December 2021, will require changes to Ireland's national legislation in this area.

EL	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?** ☒YES, fully implementing the recommendation *EYTHY (Special Institutional Support Service) (STRUCTURAL FUNDS): The Secretariat-General for Public Investments and National Strategic Reference Framework (NSRF) of the Ministry of Development and Investment drew up a sectoral NAFS for cohesion policy, the 'National Anti Fraud Strategy for Structural Actions', which it submitted to OLAF on 5 May 2014 and which was accepted in August 2014. An integral part of this is a detailed Action Plan which includes specific actions, responsibilities, timelines and results indicators. This Sectoral Strategy was updated and resubmitted to OLAF and other EU departments in March 2017. The updated Action Plan on combating fraud in Structural Actions includes all measures/actions and their evolution since 2014 to reflect the overall picture of how the Strategy is being implemented and the results achieved. Achieving the goals of the Strategy ensures that in the 2014-2020 programming period fraud in structural actions is now addressed systemically and systematically: Systemically, because the Fraud Management System is fully integrated into the Management and Control System (MCS) of the NSRF, through:* • *legislative provisions and specific measures;* • *clear procedures, workflows, reporting mechanisms and defined responsibilities.* *Systematically, because the prevention and combating of fraud is ensured through:* ✓ *the application of the relevant MCS procedures throughout the new programming period;* ✓ *the exploitation of our IT systems;* ✓ *the operation of an Internal Cooperation Network which we have created between our Managing Authorities and our Service;* ✓ *the fruitful cooperation we have with the competent national bodies and EU departments;* ✓ *the training of the agencies involved, which is being gradually extended to a wider audience; and* ✓ *continuous improvement.* *Given that the actions of the National Anti-Fraud Strategy have been fully integrated into the Management and Control System (MCS) of the OPs of the NSRF 2014-2020 (CEPOL Objective), the prevention and combating of fraud is ensured by implementing the MCS and monitoring it systematically throughout the programming period. Therefore, possible new control measures for preventing and combating fraud will now be introduced through the MCS of the OPs of the NSRF 2014-2020.* *On the basis of the above, the Greek National Strategy for combating fraud in Structural Actions (cohesion policy) is not outdated and we therefore request the removal of the relevant wording for Greece, in footnote 2 to this report and in footnote 20 to the 2018 Report on the Protection of the EU's Financial Interests.* *MANAGING AUTHORITY OF THE FISHERIES AND MARITIME OP* *Although it has not drawn up and submitted to OLAF an official text of an Anti-Fraud Strategy for the fisheries sector, the Fisheries and Maritime OP Managing Authority has integrated procedures and measures for preventing and combating fraud into the MCS of the Fisheries and Maritime OP, along the same lines as those that have been integrated into the MCS for the OPs of the ERDF, ESF and CF – as part of the 'Investment for Growth and Jobs' goal in accordance with the Greek National Strategy against Fraud in Structural Actions.*

Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?☒YES, fully implementing the recommendation

EYTHY (Special Institutional Support Service)

In January 2014, at the initiative of the Secretariat-General for Public Investments and the NSRF, it was proposed to establish a Cooperation Network for the National Strategy against Fraud in Structural Actions, linking the Secretariat-General for Public Investments and the NSRF, the Financial Audit Committee (EDEL), the Financial Crime Squad (SDOE), the National Anti-Corruption Coordinator and the General Inspector for Public Administration. This network was fully exploited in developing the Strategy and in preparing the Action Plan up until the designation of the AFCOS, through constructive meetings and by providing texts and data.

Following the official designation of the Greek AFCOS [today the National Transparency Authority (EAD)], which coordinates the authorities/bodies responsible for investigating and combating fraud, but also through the other responsibilities it has assumed (such as the coordination and operational planning of national control mechanisms), a new framework has been ensured for cooperation and information exchange, the link between administrative and judicial authorities to combat fraud and the joint response at national level. Cooperation between the Secretariat-General for Public Investments and the NSRF with the Greek AFCOS is continuous. It was particularly constructive in finalising critical issues during the planning of the MCS of the OPs of the NSRF 2014-2020 (CEPOL Objective), for handling suspected fraud and complaints about co-financed projects.

Finally, in developing the anti-fraud strategy in the Structural Funds and the Cohesion Fund, the Secretariat-General for Public Investments and the NSRF have been closely associated with the European Anti-Fraud Office (OLAF), as well as the Task Force for Greece through experts.

In this context, technical meetings and training seminars of senior staff of the Managing Authorities were held in Greece and abroad, and there was continuous cooperation with the expert group monitoring the implementation of the Action Plan.

Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?☒ YES, fully implementing the recommendation

Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;☒ YES, fully implementing the recommendation ☐

EYTHY (Special Institutional Support Service)

Given that the National Strategy against Fraud in Structural Actions is sectoral and concerns cohesion policy, continuous cooperation with the Greek AFCOS (the National Transparency Authority) has been ensured since it was set up. AFCOS is the link between the administrative authorities in the Management and Control System of the OPs of the NSRF 2014-2020 (CEPOL Objective) and the competent national authorities and bodies responsible for carrying out checks, but also for law enforcement and prosecution. The role of AFCOS for structural actions is provided for in the relevant institutional framework and is set out in detail with specific steps in the relevant procedures (and corresponding flow charts) of the MCS.

As an interface, it officially receives every case of suspected fraud detected by the MCS Authorities and forwards them to the appropriate authority/body for further investigation or prosecution. Accordingly, it is responsible for informing the MCS Authorities of the development of any suspected fraud relating to structural actions until each case is closed. Furthermore, being responsible for receiving and handling complaints about structural actions, it again plays a key role in assessing each case, forwarding it appropriately for investigation within or outside the MCS, and keeping the Authorities informed of all developments until the end of each case.EAD (National Transparency Authority)See also reply to Q.2.3.b.

Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?☒ NO

Q.2.2.a In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?☒YES, fully implementing the recommendation

This refers to risk analysis tools for the targeting of projects/operations to be submitted to specific verifications, on-the-spot checks, audits or other types of controls (as relevant). Please provide results in terms of irregularities/fraud detected during controls that have been started (also) because of risk analysis. The Irregularities Management System (IMS) provides this information, but the Member State may want to add detections that are excluded from reporting (such as detections before inclusion of expenditure in a statement of expenditure submitted to the Commission). The Member States are encouraged to provide relevant details to explain the actions undertaken or planned (in case of partial implementation) (see also question under section 2). If applicable, explain why no such action was taken.

EYTHY (Special Institutional Support Service)

The Greek Management and Control System (MCS) of the OPs of the NSRF 2014-2020, financed by the ERDF, the ESF and the CF, under the 'Investment for Growth and Jobs' goal, includes a coherent and clear framework of workflows, procedures, roles and responsibilities, based on legislative, organisational and operational interventions, for preventing and combating fraud.

The 'Handbook of MCS Procedures 2014-2020', which is applied by the competent authorities/bodies, includes procedures and measures aimed at ensuring the prevention and combating of fraud, on a systematic basis, and also the continuous improvement and reinforcement of the system. The application of these procedures is supported, inter alia, by IT tools, to which extensive reference was made in 2017 in response to the follow-up to Recommendation 4 of the 2016 Report. These tools are:

✓ *The Integrated Information System (IIS), which is the central management tool and the means of electronic data exchange among all the authorities/bodies involved (beneficiaries, managing authorities/intermediate bodies (MA/IB), Certifying Authority, Audit Authority, Commission). All the necessary information on the co-financed programmes and operations of the NSRF is recorded in the IIS, as well as data relating to the MCS procedures. Following its technological and operational upgrade, procedures and methodologies have been automated, and internal controls have been introduced to monitor the accuracy and completeness of the information (validations, etc.). The Greek AFCOS also has access to the IIS.*

✓ *The State Aid Management Information System (PSKE) and the State Aid Cumulation System*

(SACS), which have been specifically developed for State aid operations.

✓ *The Irregularities Management System (IMS).*

✓ *The Commission's Fraud Risk Assessment Tool [EGESIF 14-0021-00 (16/06/2014)], which has been adapted and optimised as regards inclusion of all the existing control measures introduced by Greece in the 'Handbook of MCS Procedures 2014-2020'.*

Please note that:

✓ *Risk analysis: In the MCS, the planning of on-the-spot checks takes into account a risk assessment methodology for operations/beneficiaries based on extraction of data from the IIS and assignment of a score to 20 risk factors/indicators (e.g. beneficiaries implementing several projects at the same time, modifications, financial corrections, etc.). To apply this methodology, specific instructions and standard forms have been issued and mechanisms have been set up that automatically score 15 of the 20 risk factors and directly calculate the overall score for each operation. The risk assessment/analysis is carried out entirely through the IIS and is applied every six months, based on the most up-to-date information available, and recorded in the online system for each operation and beneficiary.*

✓ *Reporting of irregularities/suspected fraud: The MCS authorities/bodies report irregularities and suspected fraud by providing the necessary information through the IMS, on the basis of the roles assigned to them and applying the separate procedure set out in the MCS Handbook: 'DIII_3: Reporting of Irregularities to the European Commission'. Irregularities excluded from reporting (such as irregularities detected before the expenditure was entered in a statement of expenditure submitted to the Commission) are included in the Annual Summary to be submitted to the Commission for each OP.*

The Annual Summary also indicates the corresponding corrective measures taken (reduction of amounts, etc.).

Please note that, for irregularities concerning suspected fraud in particular, the Commission is informed of the following through the IMS:

✓ *all cases of suspected fraud registered involving a contribution from the funds of over EUR 10,000 (even if this amount was not included in a statement of expenditure to the Commission);*

✓ *also, where a suspected fraud is linked to a detected irregularity but not to actual expenditure incurred, the suspected fraud is notified to the Commission where the amount, if paid, would be over EUR 10,000 in terms of contribution from the Funds (e.g. when the suspicion has been raised at the time of approval of legal commitment).*

DIRECTORATE FOR FINANCIAL CONTROL, AUDIT AND COOPERATIVES OF THE MINISTRY OF RURAL DEVELOPMENT AND FOOD (Agricultural Funds)

The Directorate for Financial Control, Audit and Cooperatives selects the undertakings to be audited as part of the annual audit programme by applying a risk analysis methodology. To ensure that the selection of undertakings for audit contributes to the effectiveness of the measures for preventing and detecting irregularities in EAGF funding, the Directorate for Financial Control, Audit and Cooperatives has improved and upgraded the 'RISK ANALYSIS' computer application.

The risk analysis includes assessment of the previous year's risk analysis, weighting of the risk factors and all relevant information regarding the approach to be followed, the techniques, the criteria and the method of implementation, in accordance with Regulation (EU) No 1306/2013 of the European Parliament and of

the Council and its implementing acts.
The Directorate for Financial Control, Audit and Cooperatives has updated the control procedures and checklists for each scheme and has drawn up a checklist for a new measure, 'exceptional adjustment aid to milk producers', with a detailed list of the risks to be checked.
The audit guidelines include the parameters examined for eliminating the risk factors.
MANAGING AUTHORITY OF THE FISHERIES AND MARITIME OP
The Managing Authority of the Fisheries and Maritime OP has taken measures which are recorded in the Fraud Risk Assessment Tool concerning the detection of irregularities, and the relevant OLAF Guidelines are also implemented.

Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?☒YES
DIRECTORATE FOR FINANCIAL CONTROL, AUDIT AND COOPERATIVES OF THE MINISTRY OF RURAL DEVELOPMENT AND FOOD (Agricultural Funds)
The results derived from using the findings of these reports are as follows:
(a) scoring and mapping as many risk parameters as possible, in order to see that the selection of undertakings best ensures the effectiveness of measures to prevent and detect irregularities;
(b) ensuring the quality of ex post checks and cross-checks of the commercial documents of those entities receiving or making payments and directly or indirectly related to the system of financing by the EAGF, or their representatives, in accordance with Regulation (EU) No 1306/2013 of the European Parliament and of the Council.

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?☒YES, fully implementing the recommendation

EYTHY (Special Institutional Support Service)
The methodology for risk assessment of operations/beneficiaries applied under the MCS for planning on the spot checks on non-State aid operations (as referred to in Q.2.2.a) includes risk factors/indicators which take account of different types of expenditure.For example:
- an operation which is financed from one Fund is examined and scored differently from an operation which is financed from more than one Fund or uses a flexibility clause;
there is a distinct 'Nature of the operation' factor, which takes into account whether the operation is a study or a technical project or a specific ECB case, or a combination of these, etc.there is a 'Method of implementation' factor, which takes into account whether the operation is implemented exclusively by means of public procurement contracts or whether it is implemented with own means or in another form (voucher) or uses simplified cost methods, etc.
EDEL (Financial Audit Committee):
All fraud risk/complaint inputs are notified to the audit authority by the MCS bodies (e.g. AFCOS, Managing Authorities), and are taken into account as additional risk factors in the risk assessment for the selection of bodies to be audited.
DIRECTORATE FOR FINANCIAL CONTROL, AUDIT AND COOPERATIVES OF THE MINISTRY OF

RURAL DEVELOPMENT AND FOOD (Agricultural Funds)
The Directorate for Financial Control, Audit and Cooperatives takes all measures in the context of auditing the expenditure of EAGF financing for market measures, with risk analysis at all levels and with specific audit guidelines which are updated and are adapted to each audited sector and beneficiary.

Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?
☒YES, fully implementing the recommendation

NATIONAL AUTHORITY FOR TRANSPARENCY (AFCOS)
✓ *The National Authority for Transparency is an independent administrative authority and is the national contact point for complaints. With a view to ensuring ease of public access to the system for receiving complaints, complaints may be submitted electronically or by mail or in person or by a representative, in the complainant's name or anonymously, in Greek or English. The Inspection and Control Unit of the Authority, staffed by 320 specialised auditors, is responsible for dealing with complaints.*
✓ *The establishment of a modern institutional framework for the protection of whistle-blowers is an action of the National Anti-Corruption Action Plan (NACAP). In that context, Greece took an active part in the European Council Working Party (FREMP – The Working Party on Fundamental Rights, Citizens' Rights and Free Movement of Persons) and before the Council's Committee of Permanent Representatives (COREPER), in the process of adopting new rules for the protection of witnesses, which were published in the Official Journal of the EU on 26.11.2019 (Directive 2019/1937).*

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?☒YES, fully implementing the recommendation
NATIONAL AUTHORITY FOR TRANSPARENCY (DIRECTORATE-GENERAL FOR INTEGRITY AND ACCOUNTABILITY – AFCOS)
As mentioned above, in accordance with the MCS 2014-2020, every time an MCS Authority detects suspected fraud, the AFCOS is responsible for forwarding the case to the competent national authorities for further investigation or prosecution. It is also responsible for informing the MCS services of the development of any suspected fraud relating to structural actions until each case is closed. At the same time, as part of the procedure for setting up a mechanism for monitoring criminal cases, and in accordance with the circulars issued by the Supreme Court Public Prosecutor's Office (2/2018 and 2a/2018), case statistics are collected from the whole country, every four months, on the progress of all pending cases relating to the prosecution of corruption, financial crime and money laundering. The data are collected, taking into account the basic principles of our justice system; they are anonymised, and include all ongoing cases of fraud against the financial interests of the European Union. The data are brought to the attention of the administrative authorities (Ministry of Justice, National Authority for Transparency –AFCOS).
At the same time, the National Authority for Transparency, in cooperation with UNODC, is working on creating a standardised statistical data collection system, which will be fully in line with the country's

	current obligations, to provide input to international organisations and bodies, including OLAF.

ES	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒NO *The Royal Decree 91/2019 has created the Advisory Council for the Prevention and Fight against Fraud affecting the financial interests of the European Union. In its first Plenary meeting, this Advisory Council created two Commissions: one for the analysis and revision of the antifraud legal framework and the other one for the elaboration and follow-up of a National Antifraud Strategy in the field of the financial interests of the EU.* *The Advisory Council for the Prevention and Fight against Fraud affecting the financial interests of the European Union, which will coordinate the elaboration of a National Antifraud Strategy through one of its Commissions, is composed by AFCOS (which holds its Secretariat), the General Public Prosecutor Office, National Police and Guardia Civil, all the Managing Authorities for structural funds, Central Paying and Coordination Agency for agricultural funds, Audit Authority, Tax Agency, Office for Asset Recovery, State Treasury (Anti-money Laundering authority) and a representation of Regional and Local entities, among others.* *Once the process for the elaboration of a National Antifraud Strategy starts, risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports will be taken into account.* *The coordination between administrative and law enforcement authorities is one the issues to be included in a future National Antifraud Strategy. Some steps are already being taken in that direction, as it is explained above* Q**.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?**☒YES, partly implementing the recommendation *Risk analysis (and their periodic update) carried out by MAs/IBs and Paying agencies include elements which are oriented to the detection of irregularities and fraud, such us the results of previous audits, new fraud patterns detected, areas in which the irregularities/fraud are more frequent according to the PIF Reports, the extent to which the specific management processes are automatised, the existence of cross checks, the linkages among companies, the possible existence of double funding, etc. The selection of operations to be verified/controlled takes into account the results of this risk analysis and thus it is concentrated in those areas where the risk of irregularity or fraud is more relevant. However, although the use of IT tools for this purpose is increasing, it is not fully widespread. None of the authorities consulted to elaborate this reply have reported any irregularities/fraud detected during controls that have been started because of risk analysis, different from those which have been reported through IMS.* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?** ☒NO**.** *In line with which was reported last year, the findings from the PIF Reports are only one of the multiple elements which are taken into account in the fraud risk assessments, so it is difficult to isolate the effects that each of those elements has as a result of its inclusion in such*

assessments.

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?☒YES, fully implementing the recommendation

As it was reported last year, fraud risk assessments were already tailored to the different types of expenditures (public procurement, grants, personnel costs, etc.), and continue being tailored during this year.

Q**.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?**

☒YES, partly implementing the recommendation

In line with which was reported last year, more Managing Authorities/Intermediate Bodies and Paying Agencies have adopted the confidential channel established by AFCOS and have fulfilled its recommendations in order to facilitate the spontaneous reporting of irregularities and fraud affecting the financial interests of the EU (see those recommendations in the last year reply to the follow-up of PIF 2017).
As a result of this, the number of allegations received through this channel has increased during 2019 with respect to 2018.
With regard to the protection of whistleblowers, the legislative proposal about which we informed last year (in the framework of the follow-up to the recommendations contained in PIF report 2017) was finally not adopted because of the general elections celebrated in Spain in 2019. According to the Spanish legal system, the celebration of general elections implies the automatic deletion of every legislative proposal that had not been approved by the Parliament at the moment in which the general elections are celebrated.
Now that the Directive (UE) 2019/1937 has been adopted, Spain will initiate the process for its transposition. Several legislative proposals have been already submitted to the Parliament by different political groups in order to regulate the protection of whistleblowers.
This does not affect to the fact that a number of "Comunidades Autónomas" have adopted laws in order to protect whistleblowers at a regional level, covering protection measures which are similar to those included in the legislative proposal at national level (which finally has not been adopted, as mentioned before).

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities? ☒YES, partly implementing the recommendation

In addition to what was reported last year and to the creation of the Advisory Council for the prevention and fight against fraud affecting the financial interests of the EU (which has been reported in the questionnaire for the PIF report 2019), the AFCOS has been working together with Guardia Civil and National Police with the objective to formalise the corresponding cooperation agreements with those entities, covering issues such as operative support and exchange of information, mutual technical advice,

	strategic cooperation and training, among others. This work is still ongoing. *The AFCOS has also been working with the State Attorney´s Office in order to formalise a procedure for the transmission of punctual information regarding the initiation, follow-up and closure of judicial (criminal) proceedings which affects the financial interests of the European Union and in which the State Attorney´s Office is participating on behalf of a national authority. This work is also still ongoing.*

FR	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?** ☒YES, fully implementing the recommendation **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?**☒YES, partly implementing the recommendation. *Our current strategy has not been developed with the police and the prosecution service. As AFCOS has no investigative powers, it did not consider itself to have the power to develop this strategy alongside the judicial and administrative authorities. Any revision of the strategy will be conducted together with the police and the prosecution service.* **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports**?☒YES, fully implementing the recommendation Q**.2.1.c. In line with what was recommended in previous years, has your national anti fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;** ☒ NO. *As AFCOS does not have any investigative powers, it did not consider itself to have the power to coordinate the treatment of individual cases with the judicial and administrative authorities. When the strategy is next revised, this coordination function will be re-evaluated.* **Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?** *YES. It can be argued that the organisations that manage EU funds have a better understanding of the types of controls needed to prevent fraud.* Q.**2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?** ☒YES, partly implementing the recommendation. *Regarding ARACHNE, these are the actions taken or that will soon be taken by the coordinating authority (CGET, Commissariat général à l'égalité des territoires (General Commission for Territorial Equality), which on 1 January 2020 became ANCT, Agence nationale de la cohésion des territoires (National Territorial Cohesion Agency)):* *- a working party meeting to develop the ARACHNE usage strategy on 3 December 2019 at the CGET;* *- an ARACHNE training session on 4 December 2019 at the CGET in particular for the Europact conference, Île-de-France, Corsica (and others); led by J.-M. Gautier from DG Employment;* *- a training session on using ARACHNE for the overseas management led by J.-M. Gautier from DG*

Employment had to be postponed due to the covid-19 pandemic and the lockdown.

The working party meeting of 3 December 2019 brought together several managing authorities so that they could present how they had got on in making use of the tool.

A relative disparity in its implementation and use became apparent. Some regions have made good progress and have even been able to use the tool on many occasions as part of their management and control activities.

Thanks to the working party meeting, it was possible to acquire an overview of the ways in which the ARACHNE tool was being used and to give a new impetus to its implementation by working on putting into place a strategy for the tool's usage.

Finally, as for the technical aspect of sending data from the various operational programmes and their integration in the tool, the ANCT is pursuing work on the the aggregator Synergie and similar programmes in order to allow regular transmission of data from the various operational programmes to feed into the ARACHNE tool.

Other actions have been taken by managing authorities themselves.

Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?☒NO

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?☒ YES, partly implementing the recommendation

From one marketing year to the next, the audit authority notes that irregularities relate primarily to the same issues: public purchasing, State aid and eligibility of expenditure. The audit authority bases its risk analysis on all the irregularities declared in the Synergie information system. This has enabled it to map risks at national level, but also at regional level, by taking all audits into account (operation and system audits) and to tailor the audit plan and supervision better to the risks highlighted in each region. Subsequently, efforts to provide support on these issues have been made: the Centre de formations des agents territoriaux (Training centre for local staff) and the CGET, the coordinating authority for ESIF (European Structural and Investment Funds) have implemented training activities, in particular on public procurement, for all those involved in managing European funds. Furthermore, the often complex problems (notably those regarding State aid) faced by the auditor examining these issues are shared and illustrated through case studies thanks to seminars and meetings, or presented to the internal control committee responsible for ruling on interpretations of the regulations.

Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?☒YES, fully implementing the recommendation

The French government adopted the circular of 19 July 2018 'on the procedure for whistle blowing by public officials within the framework of Articles 6 to 15 of Law No 2016 1691 of 9 December 2016'. This

	circular identifies public officials who are likely to be whistle-blowers in the public administration, as well as the recipients of whistle blowing reports. It also lists all the deeds or acts likely to be reported, detailed rules for whistle blowing within the context of the procedure detailed in Article 8 of the Law of 9 December 2016, as well as the measures adopted to protect and safeguard public officials who are whistle-blowers. Furthermore, it is worth noting that France must carry out the transposition of Directive EU 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law. **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?**☒YES, partly implementing the recommendation *The Ministry of Justice (DACG, Direction des Affaires criminelles et des Grâces, the Directorate for Criminal Matters and Pardons) met OLAF in October 2019 and requested to be informed of the judicial recommendations issued by the Office to the French courts. Such information could help to improve the follow-up procedures and cooperation with OLAF. Systematic and regular promotion of such cooperation will be explored when the anti-fraud strategy is next revised.*

HR	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF**? ☒NO *The Republic of Croatia has adopted two anti-fraud strategies so far. One was covering the period 2010-2012 while the other was covering the period 2014-2016, and both strategies were fully implemented. However, no new anti-fraud strategy has been adopted because of significant lack of human resources at the AFCOS service. At the same time, the AFCOS service has been faced with the constant rise in a workload.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?**☒NO *The answer to this question is 'no' because no new anti-fraud strategy has been adopted. However, the previous anti-fraud strategies were developed in close collaboration with authorities managing and using EU funds as well as with law enforcement and prosecution authorities.* **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?** ☒NO *The answer to this question is 'no' because no new anti-fraud strategy has been adopted. However, the AFCOS service has developed Irregularity and Fraud Risk Management Methodology and it has conducted risk assessments in accordance with this Methodology. Therefore, the new anti-fraud strategy would incorporate results of such assessments.* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;**☒NO *The answer to this question is 'no' because no new anti-fraud strategy has been adopted. However, the need to structure the coordination between administrative and criminal checks and investigations was addressed in the first anti-fraud strategy covering the period 2010-2012. To structure that coordination, a number of measures have been implemented: the new Budget Act has been adopted where definition of the AFCOS system in the Republic of Croatia has been formulated and which has provided legal basis for adoption of the Regulation on the institutional framework of the system for combating irregularities and fraud. In addition, the Decision on AFCOS network has been adopted and Protocols on cooperation have been signed with the State Attorney's Office, the Ministry of Interior and the Audit Authority. It has to be clarified that the AFCOS Network in the Republic of Croatia gathers representatives of law enforcement and prosecution authorities, as well as authorities with specific expertise (e.g. in public procurement).* **Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?**☒ NO

Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?☒YES, fully implementing the recommendation

Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?☒YES

The Ministry of Regional Development and EU Funds is the Managing Authority (MA) for Operational Programme Competitiveness and Cohesion 2014-2020. MA establishes effective and proportionate measures to combat fraud, taking into account the identified risks. All management and control system bodies (MA, Coordination body, Intermediate bodies level I (IB I), Intermediate bodies level II (IB II), Certifying authority (CA), Audit authority) carry zero tolerance policies to fraud and corruption, and accordingly MA, IB I, IB II and CA carry out fraud risk assessment for the purpose of fraud prevention, detection and taking of necessary corrective measures. MA collects mentioned assessment, while the Ministry of Finance is responsible for processing and analysing the obtained results, in accordance with the designated obligations.

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?☒YES, fully implementing the recommendation

The Common National Rules (CNR) that are obligatory at the operational programme level for all management and control system (MCS) bodies (Part 10: Risk Management; chapters 8-11) incorporate fraud risk assessment principles from Guidance Note on Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures (http://ec.europa.eu/regional_policy/en/information/publications/guidelines/2014/fraud-risk-assessment-and-effective-and-proportionate-anti-fraud-measures). According to the abovementioned chapter of the CNR, MCS bodies are obliged to conduct annual fraud risk assessment, while the Ministry of Finance is responsible for processing and analysing the obtained results. In addition, the mentioned fraud risk assessment is facilitated with supporting documents (guidelines) and templates provided within the CNR to enable more precise definition and recognition of any possible fraud.

Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative *journalism?* ☒YES, fully implementing the recommendation

Croatian AFCOS Service is not authorised for conducting administrative investigations/checks. However, it coordinates competent authorities to process irregularity alerts or suspected fraud as soon as possible. This means that received alerts are sent to the competent management and control system body (irregularity reporting system body) with a request to send written observations regarding the alert as well as profs which support those observations. In case of suspected fraud, alerts are forwarded to the State Attorney's Office and the Ministry of Interior. Nonetheless, the AFCOS Service cannot measure the real effect of its work (i.e. coordination activities) because it relies on written observations submitted by competent

management and control system bodies (irregularity reporting system bodies) and it does not check the substance of the case. The Irregularity Management System (IMS) has 8 cases where irregularities have been established based on the information received from informants, out of which two cases relate to suspected fraud. With regard to the protection of whistle-blowers, the Act on the Protection of Whistle-blowers was adopted on February 8, 2019 and came into force on July 1, 2019 (OG 17/2019).

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?☒YES, fully implementing the recommendation

If the word 'promoted' stands for encouraging and facilitating, than the following measures can be listed:

- Regulation on the institutional framework of the system for combating irregularities and fraud has been adopted. This Regulation defines AFCOS as a system comprised of 1) administrative authorities (irregularity reporting system bodies/management and control system bodies), 2) law enforcement and prosecution authorities, as well as authorities which have a specific expertise (AFCOS network), and 3) a coordinative authority (AFCOS service).

- Decision of AFCOS network has been adopted

- Protocols on cooperation have been signed with the State Attorney's Office, the Ministry of Interior and the Audit Authority

- meetings have been organised between administrative authorities (irregularity reporting system bodies/management and control system bodies) and law enforcement and prosecution authorities, or authorities which have a specific expertise (AFCOS network) in cases where administrative authorities need expert opinion (advice) from law enforcement and prosecution authorities, or authorities which have a specific expertise.

With regard to educational activities that would encourage and facilitate cooperation between judicial and administrative authorities, no such activities were organised in 2019 due to significant lack of human resources.

IT	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒YES, fully implementing the recommendation **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?** ☒YES, fully implementing the recommendation. Q**.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?** ☒ YES, fully implementing the recommendation **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;** ☒YES, fully implementing the recommendation **Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?** ☒ YES *In the fight against Fraud, Italy is among those countries than have an efficient strategy and effectively pursue the largest number of crimes against European funds. To take just one, for the Programmes owned by the Agency for Territorial Cohesion – PON Città Metropolitane 2014/2020 and PON Governace e Capacità Istituzionale 2014/2020 it was established (for each Programme) the Fraud Risk Assessment Team which provided to the formal adoption of risk assessment tools.* **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?**☒YES, fully implementing the recommendation *The Managing Authorities, generally, have established a Fraud Risk Assessment Task Force and a Checks Quality Review Task Force, in addition to implementing the ARACHNE system with assistance from the Ministry of Economy and Finance/Auditing Authority.* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?**☒YES *Overall, the use of findings from PIF allowed to improve the "Control" system making it among the most effective and efficient.* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?**☒YES, fully implementing the recommendation **Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism**?☒YES, fully implementing the recommendation *Pursuant to Italian legislation, all national public administrations, under which the Managing Authority operates, have implemented a comprehensive whistleblowing protection system. The MA itself routinely receives reports from whistleblowers, which are always investigated, while ensuring that the identity of the whistleblower is not disclosed.* **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities**?☒YES, fully implementing the recommendation *The Managing Authority will always respond to any request from a national judicial authority, while at the*

	same time monitoring Court proceedings which are related to irregularities in the Operational Programme. It should be noted that Italian judicial authorities are independent from the Civil Service; moreover, proceedings will often be classified. The cooperation between administrative authorities is mandated by Italian law.

CY	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF**?☒NO *Currently, the House of Parliament is under discussion of the legislation for the function of the Independent Authority against Corruption and Fraud. The Independent Authority will have several functions including investigation and reporting. The new Independent Authority will undertake the role of AFCOS. It is worthy to note that, there is already an Anti-Corruption policy, however the Anti-Fraud Strategy will be covered, through the new legislation.* **Q.2.2.α. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?**☒YES, partly implementing the recommendation *Our Risk Analysis process, takes into account among other factors, the results of previous year verifications and on-the-spot checks, the frequency of the errors identified in each project, the nature of the projects, nature of beneficiaries and type of expenditure. This information is consolidated at Fund Level and is taken into account at the sampling process. Therefore, high risk areas are more likely to be selected for verifications or on-the-spot checks.* *Additionally, the "Summary of Errors" (SoE), which is annually submitted to the EC through the submission of the accounts, is used to document all the irregularities identified through several verifications, including cases which may be excluded from reporting because these have been detected before the submission of the payment claim. The SoE of previous year is taken into account in order to determine the verification strategy in the next year.* *Further to the above, a new development is the access to the electronic platform of the Department of Registrar of Companies and official Receiver has been provided to authorised officers of the Verifications and Certification Directorate, through which companies' information can been identified. This tool allows the authorised users to identify any relationships between corporate beneficiaries and/or its representatives (e.g Directors) and shareholders, which can be used to assess whether there is any potential conflict of interest in cases of awarding contracts by Beneficiaries funded by ESIF funds.* 2. Risk Analysis **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?**☒YES *Risk assessment has been incorporated in all administrative and on the spot procedures undertaken by responsible bodies involved in programmes under shared management in the areas of Cohesion Policy, Fisheries and Aid to the Most Deprived. E.g. Risk assessment methodologies are incorporated in procedures for selecting procurement procedures in order to perform administrative verifications regarding the legality and regularity of the tender notice, evaluation and assignment procedures.* *Risk analysis is also used in order to select transactions to verify in terms of payment claims submitted by*

beneficiaries with a large number of supporting documents, or during on the spot controls for measures with a large number of final recipients.

Risk analysis incorporates data on the nature of beneficiaries, the nature of projects and the type of expenditure involved, based on ex-ante assessment of the associated risk to each category and incorporating results of previous verifications and audits.

Additionally, through the preparation of SoE and Typology of Errors (common typology of errors), we can identify the frequency of errors in each type of error and target the high risk areas in order to proceed with enhanced control testing and verifications in the next year.

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?☒YES, fully implementing the recommendation

Information regarding staff involved in co-financed projects has been incorporated in the MIS used for the management of four shared management programmes covering the areas of Cohesion Policy, Fisheries and Aid to the Most Deprived. Staff cost has been assessed as a high risk area for fraud during the fraud risk self-assessment exercise undertaken by the responsible authorities. The information in the MIS will be extracted in reports in order to identify trends and used in the framework of administrative and on-the-spot controls. This function is in progress and is gradually implemented.

3. Horizontal issues

Q**.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?**☒NO

Whistle-blowers regulation is yet to be released by the House of Parliament.

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities? YES, fully implementing the recommendation

Enhanced cooperation between judicial and administrative authorities exist in cases of detected irregularities which may result to a suspicion of fraud or established fraud. Any other types of irregularities are handled within administrative authorities. The Legal Department of the Cyprus Government and specifically the European Union Law Section of the Attorney General together with Cyprus Police work closely with AFCOS. Especially in the event of an economic operator resists in any control (performed either by OLAF or VCD or IB), and authorities other than administrative are required in order to be able to proceed with the on-the-spot checks, then the three authorities liaise between them and if required the check is performed at the economic operator premises at Police presence. In other cases, Banking Judicial Disclosure Order was necessary in order for OLAF to be able to obtain any necessary information by the Economic Operator and this has been achieved through close collaboration between the Legal Department, Cyprus Police and OLAF.

LV	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒YES, fully implementing the recommendation *First National Anti-fraud Strategy and Action plan (NAFS) for period 2017 - 2019 was adopted on January 16, 2017. Action Plan has been successfully implemented and in the end of 2019 AFCOS working party started to work on New national anti-fraud strategy and Action Plan covering period from 2020 – 2022. It is expected that new Strategy will be adopted by Government (Cabinet of Ministers) in the first half of 2020 and afterwards communicated with OLAF.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?**☒YES, fully implementing the recommendation *All AFCOS Council has been involved in drafting NAFS. Firstly, with survey about measures, which should be included in NAFS, afterwards, with concrete working party which drafted NAFS project. NAFS Action Plan includes the most important measures in field of protection of EU financial interests, which should be taken in upcoming years. AFCOS Council involves institutions from all Fraud cycles, including, law enforcement and prosecution services.* **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?**X YES, fully implementing the recommendation *Managing authorities (and other institutions) are regulary working on improvements of risk analysis and implementation of recommendations. Therefore, internal strategies and other documentation is regulary updated and improved. NAFS is drafted on actual needs from institutions involved in AFCOS Council; therefore, NAFS includes those measures, which haven't been stipulated in other legislative acts.* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;**XYES, fully implementing the recommendation *In process of implementation NAFS Action Plan, OLAF assistance Law was drafted in order to ensure effective cooperation with OLAF (more information in PIF questionnaire). During this process, main question was to find a best way to assist OLAF during administrative investigations and how to structure coordination between criminal and administrative investigations. During the process of updating NAFS, this question is actualised once more with aim to implement OLAF assistance Law in practice, as well as strengthen cooperation between AFCOS Council members via educational activities.* Q**.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?** XYES *One of measures included in NAFS for period 2017-2019 was social informative campaign #FraudOff!. In*

ordered to better understand which would be the focus themes for campaign, AFCOS every year (starting from 2017) carries out a study on opinion of society on the level of fraud and other related questions. This helps to understand not only results of campaign #FraudOff! but also impact of all NAFS. Final results (for NAFS period 2017-2019) will be available at the end of March, 2020.

We can see from study carried out at beginning of 2019 that overall confidence in public administration in the prevention of fraud and corruption is very low, but compared to previous years' studies, this indicator has increased dynamically over the years (2017.- 9%, 2018.- 11%, 2019.- 13%).

Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?☒YES, fully implementing the recommendation (Ministry of Finance, MA for Structural funds)☒YES, partly implementing the recommendation (Ministry of Agriculture, MA for agriculture and fisheries)

This refers to risk analysis tools for the targeting of projects/operations to be submitted to specific verifications, on-the-spot checks, audits or other types of controls (as relevant). Please provide results in terms of irregularities/fraud detected during controls that have been started (also) because of risk analysis. The Irregularities Management System (IMS) provides this information, but the Member State may want to add detections that are excluded from reporting (such as detections before inclusion of expenditure in a statement of expenditure submitted to the Commission). The Member States are encouraged to provide relevant details to explain the actions undertaken or planned (in case of partial implementation) (see also question under section 2). If applicable, explain why no such action was taken.

Ministry of Finance, MA for Structural funds:

One of the functions of MA is verifications over management and control system, which include controls over delegated functions of Intermediate Bodies by overseeing and revising their control system and checks. Major MA controls are - procurement ex-ante controls, eligibility and payment claim verification, on-the-spot verifications, controls of process of contract/agreement modifications as well as revise of procedures of Intermediate Bodies. Planning of MA controls of delegated function is based on the risk-cantered approach, taking into account risky spheres, which were identified during the time of previous checks. For verifications MA is using not only publicly available data bases, but also European Commission's ARACHNE information system as an additional inspection tool in cases when the possibility of fraud exists within the process of checks, and MA ensures that Intermediate Body is using ARACHNE information system during their provided checks as well.

Ministry of Agriculture, MA for agriculture and fisheries: Intermediate body - The Rural Support Service uses its IT system tools, incl. a list of risk clients, links to other external systems, area satellite imagery and atypical case studies.

Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?☒YES (Ministry of Agriculture, MA for agriculture and fisheries)☒NO (Ministry of Finance, MA for Structural funds and Ministry of Welfare, MA for FEAD)

Ministry of Agriculture, MA for agriculture and fisheries:

Intermediate body - The Rural Support Service has identified individual cases that have allowed the detection of irregularities and the prevention of undue payments.

Ministry of Finance, MA for Structural funds:

Regarding the fraud and corruption risk assessment in the monitoring and control system of the Operational Programme for the Implementation of the European Structural and Investment funds, practical fraud risk self-assessment tool (based on Annex 1 of the Commission's guidance EGESIF of 16 June 2014 "Programming period 2014-2020 Guidance note on fraud risk assessment and effective and proportionate anti-fraud measures") is used.

The fraud risk self-assessment tool targets the main situations where key processes in the implementation of the programme (selection of applicants; implementation and verification of the operations; certification and payments) could be most open to manipulation by fraudulent individuals or organisations.

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?☒YES, fully implementing the recommendation (Ministry of Finance, MA for Structural funds and Ministry of Agriculture, MA for agriculture and fisheries) ☒NO (Ministry of Welfare, MA for FEAD)

Ministry of Welfare, MA for FEAD:

Set up internal risk management and anti-fraud control system in the managing authority, clearly defining the roles and responsibilities of personnel in the implementation of the activities, avoiding any conflict of interest in the decision-making process, ensuring at least two participation in decision making and the person responsible for the supervision of operations to be supported and ensuring FEAD beneficiaries of the awareness of the institutions involved in the management of the FEAD readiness ensure the risk management process and capacity to fight fraud.

The institutions involved in the management of the FEAD shall take the measures necessary to prevent and detect potential risks, including fraud. The risk management established for expenditure shall be applied uniformly to all types

Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?☒YES, fully implementing the recommendation

Whistleblower Protection Law entered in force on May 1, 2019. Thus, public and private legal entities introduced an internal alert system and developed procedures for evaluating external alert reports. The objective of the law is strengthening of whistle-blowers protection in Latvia and to facilitate alarm sounding in the interests of the society on various irregularities. For example, the Rural Support Service received 2 alarms reports during this time, which were properly evaluated but did not confirm the facts. In addition, focus theme for 2019 in social campaign #FraudOff! was – Reporting culture. Within the

campaign we communicated with society about reporting positive effects and necessity in order to fight fraud and corruption. Reporting tool was created where individuals can report about different irregularities in easy and understandable way. Tool is situated in website www.atkrapies.lv

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?☒YES, fully implementing the recommendation

AFCOS Council is made as a network, which involves institutions from all fraud cycles. Therefore, we have meetings where all institution involved in protection of EU financial interests, meets at least twice a year. Many cooperation aspects are discussed during those meetings.

In 2019, there were several inter-institutional meetings organised between administrative bodies in EU funds and law enforcement bodies within concrete criminal cases. Those meetings and exchange of information are essential, not only to take appropriate administrative measures in project, but to assist investigation in general.

And, of course, training programmes regarding cooperation structure which are designed in close collaboration between investigation authorities and administrative institutions. Aim of those trainings is to help institutions better understand each other's work and to find best way for cooperation on daily basis. These kind of educational activities were carried out on 2018 and 2019.

LT	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?** ☒NO

LU	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF**?☒NO The preparation of the LU anti-fraud strategy document is in progress. In any event, risk management through the collection and analysis of the fraud related data is an ongoing process that is enhanced each time a fraud case is discovered. The managing authorities are in charge of inputting the data in the IMS. There is an ongoing cooperation between national stakeholders and the competent Commission services. In addition, several managing authorities already implemented internal policies describing the steps to follow in case of fraud detection. In case of fraud suspicion followed by an investigation, AFCOS is kept informed on the exchanges the managing authority has with OLAF and the Public Prosecutor's Office. Pending finalisation of the strategy, implementation of the recommendations by national stakeholders is ongoing. **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?** ☒YES, fully *The managing authority of the European Regional Development Fund (FEDER), the Ministry of Economics, the managing authority of the European Social Fund (ESF), the Ministry of Labour, as well as the INTERREG programme, managed by the Ministry for Spatial Planning, all implemented the Arachne tool. This was done in tight collaboration with the Commission's services. The latter helped them to enhance management of their internet platforms, used by promoters to upload information regarding, inter alia, expenses. The managing authorities use the internet platform as a management control tool for their projects as all the information is centralised on it. Collected information is exported in Arachne. INTERREG uses in addition a Risk Assessment Tool in the framework of the establishment of their management control system. Its procedures are adapted based on the results from the Risk Assessment Tool. In addition, INTERREG programme elaborated more tools to report on fraud, like a formulary to notify first level controllers. Controls are made onsite. The Ministry of Agriculture, the managing authority for the European Agricultural Fund for Rural Development (FEADER) and the European Agricultural Guarantee Fund (FEAGA) uses the IMS in the framework of its activities. Same for the managing authorities of FEDER and ESF. The Inspectorate General of Finances, which is also ESF's Audit Authority, can access ESF's IMS and ESF's internet platform. The latter is used for the daily management of the ESF and its projects. The application has a back office for the managing authority and a front office for the project owners. Most of the common tasks are done through or with the support of the platform: deposit of new projects, reporting of data (i.e. payment claims, follow-up of indicators, monitoring of, first level control,…). All available data on ESFprojects is centralised on this platform and it ensures transparency and a possible audit trail. When accessing it, the Inspectorate General of Finances can get all the available information needed for their second level control. ESPON does a risk analysis and in its programme documents include that the Single Beneficiary of the programme is, in addition, obliged to have a risk analysis that is updated every year. The managing authority checks the risk analysis of the Single Beneficiary on a yearly basis during the quality checks on the spot. Based on the results of the management authority's verifications and of the quality checks, the decision is taken* whether there is a need *to update the programme level risk analysis. Arachne was not an option for ESPON having only one beneficiary for the programme. This has been duly discussed with Commission's services. It has been notified that it was not possible to grant access to Arachne to the Single Beneficiary since it was not useful for the programme.*

Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?☒NO

If yes, please provide a summary of the results achieved. If no, please provide the reasons. In case of ESF there is a very low margin for error. Expenses are under EUR 10,000. FEDER only disburses to public entities, which are all risk assessed by our national court of auditors. For INTERREG, ESPON and FEAGA & FEADER there are no findings.

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure? ☒YES, fully implementing the recommendation

In the framework of the ESF, a simplification of cost options for the projects exists, so as to reduce administrative burden and to focus on the outputs and results of the projects instead of limiting the checks of the application of accountability rules. This has been agreed with the Commission's services. As for FEDER there is no need for since the managing authority only disburses to public entities, which are all risk assessed by our national court of auditors. In 2016, following a fraud discovery, the Ministry of Agriculture, the managing authority for FEAGA and FEADER, created the "Procedure and Special Investigations service – service Procédure et Enquêtes Particulières (PEP)", whose mission is to prevent fraud cases. Before that a guidance note for Premium managers to prevent fraud in the agricultural sector has been created. The reason behind it was a scam which was discovered in 2013 following an internal administrative audit. Following that incident, the Ministry of Agriculture fundamentally reviewed its external and internal control system. Several measures /safeguards were taken or reinforced since then. This procedure is one of them. An alert system has also been set up in (the framework of article 58 of regulation 1306/2013) to detect facts that may indicate fraud or attempted fraud. In case of INTERREG, the expenditure is always 100% controlled, but the manual of the program insists on paying particular attention on the staff cost and on external expertise, in particular to the services that require to respect public procurement procedures. A risk chart has also been created and is updated on a 2-years basis (last time in 2018), abiding by the Commission's guidelines. For ESPON the risk approach has been tailored since it mainly focuses on public procurement. The explanation is the following: when the risk analysis at programme level was implemented the ESPON team detected a series of risks mainly related to the implementation of public procurement. On this basis, specific provisions where included in the programme implementation guidelines for the single beneficiary: (i) obligation of having a project specific risk analysis is updated every year, (ii) separation of function, (iii) need for an independent lawyer verifying the implementation of public procurement, (iv) cooperation on rotation basis of project expert in charge of the content and the financial expert in charge of the administrative part of the procurement, (v) rotation principle of project experts to avoid that they work with the same service providers; (vi) definition of the role of the managing authority as observer in certain procurements or in certain phases of the procurements.

Q**.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?** ☒YES, partly implementing

The managing authority in charge of FEAGA and FEADER, the Ministry of Agriculture, set up an internal whistle-blowers policy following the discovery of a fraud case in 2015. ESPON has introduced in its internal manual specific provision for whistle-blower. The INTERREG program has an email address to

	which whistle-blowers can report. FEDER and ESF do not have specific measures to protect whistle-blowers, however, with reference to article 23 paragraph 2 of the Code of Criminal Procedure, civil servants are obliged to report any suspicion of fraud or irregularity to the Public Prosecutor's Office. International standards of auditing and checklists are used by the managing authorities in the framework of their reporting. **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities**? ☒YES, fully implementing the recommendation *The managing authorities report to the Public Prosecutor's Office any suspicion of fraud. AFCOS is also in contact with the Public Prosecutor's Office as often as required and in line with applicable legislation. In March 2019, a member of Luxembourg's AFCOS and one prosecutor, covering OLAF related issues, jointly attended a conference in Bucharest, called "EU Anti-Fraud Partners' Meeting". The latter was organised by Romania's Fight against Fraud Department – DLAF. The aim of the event was to provide the adequate ground for exchanging information, experience and best practices on EU anti-fraud issues, especially in the context of the future cooperation between Member States, OLAF and EPPO. Further, in November 2019, an "EU Conference on investigating frauds and corruption affecting the financial interests of the European Union" in Bucharest has been attended by a representative of our Inspectorate General of Finances.*

HU	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒YES, fully implementing the recommendation *Hungary has had an anti-fraud strategy since 15 June 2015, which has been communicated to OLAF.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services**?☒YES, fully implementing the recommendation *The Anti-Fraud Strategy was drawn up by the Prime Minister's Office, responsible for the use of EU funds that time in collaboration with participants in the network of institutions involved in performing tasks related to development policy.* **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports**? ☒YES, fully implementing the recommendation *A meeting of the Fraud Risk Assessment Coordination Working Party was held. The Managing Authorities (MAs) drew up action plans and then performed their risk assessments according to those plans. The Coordination Body assessed and analysed the integrity and corruption risks and drew up an action plan to deal with them. Implementation of these measures is ongoing.* *An Order of the Minister of State for Administrative Affairs at the Prime Minister's Office on the procedure for collecting and investigating reports of abuses, infringements and integrity and corruption risks associated with the operations of the Coordination Body was adopted. Following adoption, it will be applied on an on-going basis. Audit trails have been updated centrally in line with the amendments made to Government Decree No 272/2014.* The national strategy has been reviewed since 2016. *The Managing Authorities identify and assess the risk of fraud on the basis of the EGESIF_14-0021-00 guidance document published by the Commission, for which the Hungarian authorities have drawn up methodological guidance.* *The main processes inspected as part of the assessment were:* • *applicant selection;* • *operation implementation and verification;* • *certification and payments;* • *public procurements conducted directly by the Managing Authorities.* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;**☒YES, fully implementing the recommendation *The national strategy has been reviewed since 2016.* *The Management and Security Department of the Ministry of Innovation and Technology deals with the registration of criminal complaints related to EU funds, ongoing criminal cases and whistleblowing. With regard to ongoing criminal cases, the Department keeps in regular contact with the law enforcement authorities and the Managing Authorities. Government Decree No 272/2014 of 5 November 2014 contains*

detailed procedural rules. A special functionality was developed in the section of the Hungarian Development Policy Database and Information System (FAIR) dealing with Union support. Its aim is to prevent fraud and abuses and detect it early (the 'fraud prevention functionality'). The functionality is being constantly improved in the light of emerging needs: In 2018, it was expanded with a question about indicators.

According to the model protocol for irregularity procedures issued by the Coordination Body, cases of irregularities registered as suspected fraud must be recorded separately, so they can also be filtered using the FAIR EUPR irregularity module.

Cooperation with the National Tax and Customs Administration is ongoing. Contact was also made with the National Office for the Judiciary, as a result of which a whole-day training course entitled 'Fiscal fraud and related crimes' was held for the network of institutions handling Union support. The aim of the training was to present case-law.

The Hungarian Competition Authority and the Public Procurement Authority held a training course for the network of institutions handling Union support as part of a similar training course in 2018.

Also, in November 2019, training was held on the use of the Arachne system, involving a presenter from the European Commission.

In 2019, OLAF's Anti-fraud coordination service (AFCOS), in cooperation with the Coordinating Body, provided a training course to the network of institutions handling Union funds on a total of two occasions, entitled 'Fraud prevention in the field of EU development policy'.

Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?☒NO

Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?☒YES, fully implementing the recommendation

This refers to risk analysis tools for the targeting of projects/operations to be submitted to specific verifications, on-the-spot checks, audits or other types of controls (as relevant). Please provide results in terms of irregularities/fraud detected during controls that have been started (also) because of risk analysis. The Irregularities Management System (IMS) provides this information, but the Member State may want to add detections that are excluded from reporting (such as detections before inclusion of expenditure in a statement of expenditure submitted to the Commission). The Member States are encouraged to provide relevant details to explain the actions undertaken or planned (in case of partial implementation) (see also question under section 2). If applicable, explain why no such action was taken. Arachne software has been installed in every Managing Authority which deals with ERDF, ESF and CF. How actively Arachne is used depends on the group of beneficiaries a Managing Authority has. Managing Authorities which typically cooperate with the budgetary institutions do not use Arachne, as the FAIR EUPR fraud prevention functionality provides them with sufficient information. Data obtainable using Arachne software enables ownership relationships among companies, conflicts of interest and concentrations to be checked and SME status to be verified. In 2017 we ran a training course entitled 'A general presentation of the Arachne

system, and a presentation of risk categories and risk indictors' with 39 participants, at which the presenter sent by the Commission described how the system is used. Another training session was held in November 2018. Use of the Arachne system is regulated by the Methodological guidance for the application of the ARACHNE IT system to ensure evaluation of the risk of fraud in the implementation of the 2014-2020 programming period. Test data have already been dispatched to the ARACHNE system and, on the basis of the Commission's feedback, Hungary has made the requisite corrections. We sent you live data for the first time in mid-October 2018 and most recently at the end of 2019. The application of ARACHNE user authorisation can be initiated by anyone whose remit justifies it, by filling in Annex 1 to the ARACHNE system access management regulation. The number of authorised persons is continuously expanding in accordance with demand – currently 128 people have access. 81 users from managing authorities and 47 from the audit authority have authorisation.

Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?☒YES

When examining the public interest reports placed on the public interest reporting system operated by him (www.anti-lop.hu), the minister responsible for the use of EU funds may request information and data from the managing authorities and may notify of a suspected irregularity; the managing authorities send this information and data to the minister responsible for the use of EU funds within five working days of receipt of the request for information on any infringement proceedings that may have been initiated. The Minister takes the necessary measures on that basis.

The regulation on the operation of the reporting system and protection of the whistle-blower was issued under number SZBF/1/6/2/2016: 'Order of the State Secretariat for Administrative Affairs of the Prime Minister's Office on the procedures for collecting and investigating reports on abuses, infringements and integrity and corruption risks associated with the operations of the Prime Minister's Office'. The audit trails were updated centrally by the deadline, pursuant to the amendments to Government Decree No 272/2014.

In addition to the above, training was provided to colleagues, the Managing Authorities drew up their own anti-fraud policy, and Arachne software was installed in each and every Managing Authority. Discussions on experience in analysing fraud risk took place within the Fraud Risk Analysis Coordination Working Party.

The use of a specially designed special fraud prevention functionality in the part of Hungary's IT system (FAIR) dealing with EU funds (EUPR) is ongoing; this interface provides information on every project, with the aim first and foremost preventing fraud and abuse and enabling early detection.

The ARACHNE system: use of the fraud prevention system designed by the Commission is continuous in investigations where it provides information in addition to that provided by the national IT system (such as on ownership relationships, for instance).

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?☒YES, fully implementing the recommendation

The Managing Authorities identify and assess the risk of fraud on the basis of the EGESIF_14-0021-00 guidance document published by the Commission, for which the Hungarian authorities have drawn up methodological guidance. The main *processes inspected as part of the assessment were:*

- *applicant selection;*
- *operation implementation and verification;*
- *certification and payments;*
- *public procurements conducted directly by the Managing Authorities.*

Q**.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?**☒YES, fully implementing the recommendation

Citizen's complaints are of considerable help in detecting cases and identifying irregularities – the forum for those is the website www.anti-lop.hu, where citizens can report abuses anonymously with a view to protecting their privacy. Furthermore, requests sent to the customer service of the coordination body, by which an informant may request information and data from the managing authorities and notify of a suspected irregularity, are also examined; the Managing Authorities send this information and data to the minister responsible for the use of EU funds within five working days of receipt of the request for information on any infringement proceedings that may have been initiated. The minister takes the necessary measures on that basis. The regulation on the operation of the reporting system and protection of informants was issued under number SZBF/1/6/2/2016: 'Instruction of the State Secretariat for Administrative Affairs of the Prime Minister's Office on the procedures for collecting and investigating reports on abuses, infringements and integrity and corruption risks associated with the operations of the Prime Minister's Office'. The data processing obligations associated with the Managing Authorities' reports are set out in the Single Operations Manual – they have no separate procedures.

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?☒YES, fully implementing the recommendation

Currently the Management and Security Department of the Ministry of Innovation and Technology is responsible for the coordination of official requests relating to the use of EU funds and whistleblowing. Thus the entire criminal inquiry referred to the Managing Authority is concentrated in one department. This reinforces the personal contacts between the authorities and administrative bodies, increases transparency, reduces the number of parallel investigations and facilitates the detection and prevention of crimes associated with the use of EU funds. In addition, cooperation between the National Tax and Customs Administration, the Hungarian State Treasury, the National Office for the Judiciary, the Hungarian Competition Authority and the Public Procurement Authority is ongoing.

MT	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒YES, fully implementing the recommendation *Malta's Reply: The Maltese 'National Anti-fraud and Corruption Strategy' tabled in Parliament by the then Prime Minister of Malta in 2008 was also communicated to the European Commission/OLAF.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?** ☒YES, fully implementing the recommendation **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?**☒ NO *Malta's Reply: The Strategy is currently in the process of being updated as necessary.* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;** ☒ YES, fully implementing the recommendation **Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?** ☒ NO **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?** ☒ YES, fully implementing the recommendation **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?**☒ NO - *No results are available.* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?** ☒ YES, fully implementing the recommendation **Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?** ☒ YES, fully implementing the recommendation *The Protection of the Whistleblower Act, which was adopted in July 2013 and made applicable by a ministerial decision of 15 September 2013, establishes a system of internal and external reporting channels to be used by persons disclosing in good faith corrupt practices and other suspicious behaviour. The act allows various forms of protection for the whistleblower, including immunity from criminal proceedings, in which case the Attorney-General acting in consultation with a Judge of the superior Courts and the Commissioner of Police may grant such immunity where the reporting person was him/herself involved in criminal acts.* *Whistleblower Act (Chapter 527 of the Laws of Malta) applies in the context of an employer – employee relationship. The terms 'employer' and 'employee' are specifically defined in the Act.* **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?**☒ YES, fully implementing the recommendation

NL	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒NO *There is a procedure to come to a combined outline of all antifraud policy for the means in shared management. A next step is a transformation to an actual strategy.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?** ☒YES, partly implementing the recommendation *Strategic cooperation with all bodies is in place and is part of the procedure to come to an outline of all antifraud policy and measures.* **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?** *The Netherlands has taken into account the risk analysis conclusions of the previous PIF reports. Not in the NAFS, because it is not implemented yet, but per fund risk analysis is in place.* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;** *The need to structure between administrative and criminal checks has taken into account in the policies of the individual funds in shared management (but not in NAFS because it isn't implemented yet).* **Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?** *Not implemented yet* **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?** ☒YES, fully implementing the recommendation *After several pilot projects in previous years on the use of ARACHNE, this year ARACHNE is fully operational. To this end, project data was exchanged with ARACHNE. This has not led to detection of fraud.* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?**☒NO **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?** ☒NO Risk analysis is already sufficient to detect fraud. **Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?** ☒YES, fully implementing the recommendation *No changes compared to 2018. At that time it had already been implemented.* **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?** ☒YES, fully implementing the recommendation *No changes compared to 2018.*

AT	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?** ☒YES, fully implementing the recommendation *No details.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?** ☒NO *No details.* **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?** ☒NO *No details.* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;** ☒YES, fully implementing the recommendation *No details.* **Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?** ☒YES *No details.* **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?** ☒YES, fully implementing the recommendation *No details.* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?** ☒NO *No details.* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?** ☒YES, fully implementing the recommendation *No details.* **Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?** ☒NO *No details.* **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities**? ☒NO *No details.*

PL	**2.1 Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒NO *A national anti-fraud strategy has yet to be drawn up. Poland has yet to take a decision on drawing up a strategy, as the European Commission has imposed no obligation to do so. Before any such strategy is drafted, the competent national bodies will analyse the pros and cons of adopting such a tool. In the meantime, the managing authorities of the individual operational programmes have established anti-fraud documents. Depending on the approach adopted and the nature of the programme, such a document is termed 'strategy', 'policy' or 'guidelines'. The programme approach applied allows a proper assessment of the current situation with regard to anti-fraud measures, risk assessment and the development and introduction of proportionate measures to combat fraud at the lowest possible management level.* **2.2.a In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?** ☒ YES, fully implementing the recommendation *As regards cohesion policy, successive measures have been taken to reinforce risk analysis aimed at detecting different kinds of irregularities and fraud. This is done using IT tools that simplify work and step up action in the selected fields. A 'Cross Checks' IT application is being developed for the purpose of identifying cases of double financing of expenditure incurred by beneficiaries implementing projects co-financed by Union funds.* *A machine algorithm flags up suspected cases of invoices issued by a given issuer (based on the NIP number) that may have been submitted more than once by a beneficiary and may indicate double financing of expenditure. The application is set to evolve into a larger system known as SCANER (Score-based Antifraud National Estimation of Risks), which is currently at the design stage. In addition to the 'Cross Checks' application, the system will include other applications for such purposes as collecting data from external databases such as the National Court Register, the Central Register and Information Repository on Economic Activity (CEiDG) and the report on the recruitment of personnel for projects that have been carried out. Taking into account the functionality of the tool developed and subsequent activities for its development, it is not only innovative and transparent but has the potential to become a comprehensive risk-analysis tool. Owing to the functionality and architecture of the system introduced, ARACHNE is not used.* *As regards supervision by the managing authority over the bodies involved in implementing the 2014-2020 Rural Development Programme, quarterly checks are carried out under the Ministry of Agriculture and Rural Development's control plan. The risk analysis carried out for the purposes of designing the control plan covers such aspects as the state of implementation of individual support instruments (including the amount of public money spent), the results of earlier checks and audits (including the results of checks by the Supreme Audit Office, the Agency for Restructuring and Modernisation of Agriculture, the European Commission and the European Court of Auditors), planned checks by the Paying Agency, complaints, conclusions and other reports on irregularities and the results of studies and analysis. The risk factors taken into account in this analysis are adapted to the current state of the RDP's implementation in order to identify the scope of control, the support instrument and the operator controlled as well as possible.*

Paying Agency case-handlers use a list of red flags that could warrant suspicions of fraud. After identifying red flags, the case-handlers take further measures to verify the procedures laid down or perform other appropriate checks/controls (in-depth analysis of the case). In specific cases, an analysis is also carried out on the basis of the registers and databases available to the Agency.

2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments? ☒YES

As regards data in the PIF report, information on irregularities and fraud detected are a key element of risk analysis. Another element is constituted by complaints/conclusions or other reports received by the competent bodies of potential errors/infringements. These data are taken into account in risk analysis. Since 2016 Paying Agency staff have been made more aware of fraud by:

1. the introduction of a list of red flags for the purpose of raising the awareness of Agency for Restructuring and Modernisation of Agriculture staff involved in all stages of the administrative and control cycle of anomalies (signs) that could warrant suspicions of fraud;

2. annual analysis of the risk of fraud aimed at identifying risk areas, evaluating the effectiveness of the control mechanisms deployed and, in specific cases, introducing new control mechanisms to reduce to a minimum the risk of fraud in respect of financial support granted by the Agency;

3. training for Agency staff on fraud.

2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure? ☒YES, fully implementing the recommendation

As regards cohesion policy, the sampling of expenditure and projects for control is based on risk analysis. The assumptions underlying this analysis are set out in the annual control plans drawn up for each operational programme for a given accounting year. Managing authorities also apply the risk analysis advocated in the Commission's guidelines.

On-the-spot checks are carried out by the Paying Agency on the basis of a separate risk analysis for each type of expenditure and action. An individual risk analysis is performed for each action (scheme). For every risk identified, a control mechanism is laid down along with a reference to the procedure, guidelines or circular governing the control in question and information on whether the checks are documented and whether their effectiveness is subject to regular scrutiny. The functioning of the above control mechanism for preventing fraud is verified in the course of internal control by staff from Agency headquarters.

2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism? ☒YES, fully implementing the recommendation

Polish law gives bodies managing and implementing Union funds a free hand when it comes to voluntarily reporting potential irregularities. For instance, the Managing Authority for the Infrastructure and Environment Operational Programme has developed a reporting mechanism for the 2014-2020 programme. Irregularity reports are sent via the reporting mechanism to the e-mail address: nadużycia.pois@mfipr.gov.pl or the programme's dedicated webform: e-Nieprawidłowości [e-

Irregularities]. Note that reports received via these channels sometimes concern other operational programmes too. In that case a report is sent to the competent authority concerned (e.g. the competent managing authority) or the person concerned is informed of the body to which they should report the case.

Under the reporting mechanism for the Infrastructure and Environment Operational Programme, an initial verification is carried out by the relevant staff at the Managing Authority, who send the contents of the report (in the form of an anonymised attachment if the person making the report wishes to remain anonymous) to the unit of the intermediate body/implementing body responsible for the action concerned with a request for a detailed analysis of the possible irregularities. Once the analysis has been carried out, an implementing authority/intermediate body must inform the managing authority of the action taken to resolve the issue, including in particular handing over the case to other authorities and services, namely: the Office of Competition and Consumer Protection (UOKiK), the Central Anti-Corruption Office (CBA), the Internal Security Agency (ABW) or the public prosecution service.

A monitoring table enables the follow-up to reports on suspected irregularities or fraud to be recorded regardless of the form of those reports. Once suspicions of fraud or irregularities concerning the Innovation and Environment Operational Programme have been confirmed by the Managing Authority/Intermediate Body/Implementing Body (on the basis of an investigation launched by the law-enforcement authorities or by the Office for the Protection of Competition and Consumers on the basis of a notification by the Managing Authority for the Innovation and Environment Operational Programme), these reports are entered without delay in the Database of investigations by the law-enforcement authorities and the Office for the Protection of Competition and Consumers and fraud or suspected fraud. The Managing Authority for the Infrastructure and Environment Operational Programme monitors and evaluates the irregularity reports received. Having seen how this mechanism has worked in practice, we are considering recommending that all other managing authorities adopt the same solution.

Furthermore, national rules require administrative authorities to examine and handle complaints and conclusions within their remit. Moreover, nobody can be exposed to loss or blame for having filed a complaint or objection. To give an example of good practice in the handling of citizens' complaints, if the Managing Authority for the 2014-2020 Rural Development Plan receives an anonymous complaint, it carries out an investigation or, in accordance with the division of competences, forwards the case to the competent body with a request for an investigation into the accusations made.

The Paying Agency records all irregularities found, including voluntary repayments by beneficiaries. As regards reports to the Paying Agency concerning possible irregularities and fraud, the Agency's website announces the possibility of reporting fraud affecting aid granted by the Agency for Restructuring and Modernisation of Agriculture and corruption involving the latter Agency's staff. Reports can also be made to the Agency for Restructuring and Modernisation of Agriculture by letter or email (including anonymously).
The mailbox sygnal@arimr.gov.pl has been created for that purpose, and every report sent to the Paying Agency by letter or email is routinely verified and analysed before being investigated. In 2020 there are also plans to update the Paying Agency's anti-corruption policy to include rules on the procedure for reporting fraud, staff under pressure to behave corruptly or possessing information on corrupt behaviour by another member of staff, taking account of the legislation in force and the instruments available for their

protection.
In the period 1 January-31 December 2019 the Paying Agency and implementing bodies initiated 1182 investigations into reports of irregularities and fraud. In 2019 there were 102 fewer investigations than in 2018. At 9 January 2020 the situation with regard to reports on suspected irregularities received by the Paying Agency was as follows:

1) no irregularities were found in 378 cases,
2) irregularities were found in 59 cases,
3) proceedings are ongoing in 572 cases,
4) reports were left unexamined in 173 cases.

2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities? ☒ YES, fully implementing the recommendation

As regards cooperation between Poland's judicial and administrative authorities, there is an agreement between the National Prosecutor and the minister responsible for regional development. On the basis of this agreement, regular exchanges of data take place concerning beneficiaries of EU funds that have been the object of investigative measures. In addition, some bodies make use of the possibility to consult public prosecution service representatives if they urgently need data on specific ongoing proceedings.
At the Paying Agency, in the event of suspicions of fraud, the competent authorities are notified under the procedures adopted and in accordance with Article 304(2) of the Code of Criminal Procedure. Furthermore, draft reports on suspected crimes or misdemeanours are drawn up on the basis of the results of checks carried out by the internal control service. As regards cooperation with the law-enforcement and judicial authorities, the Paying Agency routinely cooperates with the Police, the Prosecutor's Office, the Central Anti-Corruption Bureau and the Internal Security Agency to detect fraud on the part of Agency for Restructuring and Modernisation of Agriculture beneficiaries, forwarding the requisite data and documents and organising meetings on specific cases.

PT	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**AFCOS BE (ICCF) ☒NO *The anti-fraud strategy was communicated to all actors in the management and control systems of the European Funds and was taken into account by them when designing their internal control procedures. The descriptions in the management and control systems of all the managing and certifying authorities are reviewed each year by the Inspectorate-General for Finance (IGF) - Audit Authority. As provided for by law, the anti-fraud strategy stipulates that each entity involved must prepare a risk management plan regarding corruption and related offences, which is reassessed every year.* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;**☐ X YES, partly implementing the recommendation *We would highlight the Protocol concluded between the Agency and the DCIAP (Central Department for Criminal Investigation and Prosecution) and regular cooperation of the Inspectorate-General for Finance - Audit Authority (IGF - AA), which systematically makes available its own resources to investigation teams of the Public Prosecutor's Office. In addition, specific training events were held in the field of fraud, including two events aimed at public prosecutors, in which the IGF - AA played an active part.* **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?** ☒YES, fully implementing the recommendation *The Inspectorate-General for Finance - Audit Authority (IGF - AA) uses ARACHNE, which has been instrumental in getting the other national authorities to start 'feeding' and using it.* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?** ☒NO (FEDER Bruxelles-capitale). *The findings of the PIF Reports are taken into consideration in the annual review of procedures, including in the fraud risk assessment conducted by the various actors in the management and control systems.* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?**☒YES, partly implementing the recommendation **Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?**☒YES, partly implementing the recommendation *A specific section for whistle-blowers is available on the website of the Inspectorate-General for Finance - Audit Authority (https://www.igf.gov.pt/paginas-participacao-civica/nova-participacao.aspx). The reported information is analysed and forwarded to the competent entities, which must notify the IGF, within a reasonable time, of the outcome of the steps taken. The whistle-blowers are informed of the progress of the procedures.* **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?** ☒YES, partly implementing the recommendation (FEDER wallonie) *As mentioned in Q.2.1.c, in addition to the IGF making its own resources available, the Audit Authority participates in training sessions (Lisbon and Porto) aimed at public prosecutors on 'Fraud in obtaining subsidies'.*

RO	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒NO *A draft of the national anti-fraud strategy for the current programming period was prepared, but it was not adopted in the reference period. The RO AFCOS is in the process of evaluating the updating of the draft strategy for the next programming period of 2021-2027.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?**☒YES, fully implementing the recommendation *The draft strategy was developed in cooperation with all the national bodies and authorities which have a specific role and expertise in the protection of the EU financial interests. The draft was not adopted – see answer to question Q.2.1.* **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?** ☒ YES, fully implementing the recommendation In *the draft Strategy (which was not adopted - see answer to question Q.2.1), the general objective "Strengthening the national anti-fraud system through prevention measures" was introduced and it had as a specific objective "The adoption of effective and proportionate measures to combat fraud, taking into account the risks identified". The measures that were to be taken in order to reach this objective were:* *- the adoption by the European funds Managing Authorities of the Initial Declaration of Anti-Fraud Intent;* *- identifying and assessing fraud risks;* *- developing and implementing a National Register of fraud risks;* *- the adoption of effective and proportionate measures to combat fraud, taking into account the risks identified.* *All these measures should have taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports (if the Strategy would have been adopted see answer to question Q.2.1).* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;**☒ YES, fully implementing the recommendation *In the draft Strategy (which was not adopted - see answer to question Q.2.1), the general objective "Strengthening the national anti-fraud system through prevention measures" was introduced and it had as a specific objective "Strengthening the interinstitutional cooperation in the field of the protection of the European Union's financial interests in Romania". One of the measures to be taken in order to reach this objective was "Preparation / updating of the collaboration protocols with the partner institutions"* **Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?**☒ YES *The draft strategy aimed to promote a competitive, fair and integrated business environment and reduce*

vulnerabilities and risks of fraud in the business environment. It also concerns the regional and international promotion of the anti-fraud expertise held by Romania, which offers guarantees on the loyal fulfilment of the obligations incumbent on the Member States within the single market.

Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?☒YES, fully implementing the recommendation**.** Examples from the RO authorities experience:

Ministry of European Funds

Irregularities and also, in some instances, cases of fraud are often detected as a direct consequence of using ARACHNE together with other internal methods of verification and control. However, we have, so far, not detected any irregularities and/or fraud following fraud risk self-assessment process realised by the MA.

Managing Authority for Operational Programme Administrative Capacity

AM POCA uses the ARACHNE tool in the process of evaluating operations for obtaining financing, in the process of administrative verification of public procurement, as well as in the activity of checking and finding the irregularities. However, following the use of this tool, no irregularity / fraud was identified.

Also, at the AM POCA level, the fraud risk assessment tool recommended by the EC in the Guidance Note EGESIF_14-0021-00 is used. In this regard, in May 2015, before designing the controls / verifications of the managing authority for POCA management, a first self-assessment (ex-ante) of the risks of fraud was finalised at the level of the 4 key processes and new/supplementary measures and controls were established were established, whose implementation and effectiveness have been finalised and measured respectively by specific reports. Subsequently, according to the EC recommendations regarding the frequency of self-assessments, the self-assessments of fraud risks were completed, on the basis of the existing / applicable controls / verifications at the level of the managing authority.

Managing Authority for Regional Operational Programme

In 2019, a training session was organised at the request of the Ministry of Regional Development and Public Administration, which was attended by representatives from the Irregularities Detection and Anti-Fraud Service, the Project Monitoring Directorate, the Priority Axis Contracting Service, the Procurement Verification Service and the Project Authorization Service. In the activity of the Irregularities Detection and Anti-Fraud Service, ARACHNE was used in specific cases, when it was required from the analysis of the case under review. Currently, at the Ministry of Public Works, Development and Administration level, the personnel from various departments is in the training stage, so that ARACHNE can be used as a means of fraud prevention.

Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments? ☒NO - *Examples from the RO authorities experience:*

Ministry of European Funds

As stated before in the previous PIF questionnaire (2018), the MA has not used any results deriving from the use of findings from PIF Reports, mainly due to the fact that the findings presented in the report

describe, among other things, various rules (e.g.: new rules adopted to reduce VAT fraud), different operational measures adopted by several Member States on expenditure to raise awareness, a collection of main achievements regarding detection of fraud and irregularities by some Member States etc., whereas the purpose of fraud risk assessment was intended to be a useful tool for self-evaluation, based on which the MA could easily identify new possible risks, following a careful consideration of the status quo of each internal structure within the MA.

(Completing the PIF questionnaire consists mostly in enumerating the main measures (administrative, legislative, organisational etc.) that have contributed or can contribute to a good extent to effectively protect the financial interests of the European Union, while assessing the risks of fraud means, basically, the assessment of existing controls and identifying eventually new planned controls designated to better tackle this matter.)

However, the MA fully complies with the requirements stipulated at Chapter 9. 9.2 of the final PIF report of 2018 issued by OLAF. For example, the MA has an anti-fraud policy put in place and, at the same time, provides useful information and actively participate (when requested) to meetings in order to strengthen the efforts of creating and properly implementing the national anti-fraud strategy.

Some irregularities and all cases of fraud identified by MA (through internal and/or external sources) are managed in very close collaboration with institutions that are direct responsible with criminal checks and investigations (e.g.: DLAF, National Anticorruption Directorate etc.).

The MA takes into consideration all viable external sources such as whistleblowers and tips from media. The information received form this kind of sources are carefully analysed and afterwards cross-examined by competent bodies, without disclosing, in any way, the identity of the person. The protection of personal data of the source is guaranteed by internal procedures and other specific national and EU regulations.

Given the examples provided above, The Fight against Fraud Department (RO AFCOS) took into account the conclusions from the previous PIF reports concerning the fraud risk assessment of every authority by introducing a specific objective in the draft national anti-fraud strategy – see answer to question Q.2.1.b.

Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?☒YES, fully implementing the recommendation**.** Examples from the RO authorities experience: *Managing Authority for Operational Programme Administrative Capacity*

AM POCA identified that, as a result of the use of the fraud risk assessment tool recommended by the EC, it is necessary to use the ARACHNE instrument in a specific manner regarding public procurement expenses and to use a different approach of the instrument as far as the process of evaluating financing operations is concerned.

Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?☒YES, fully implementing the recommendation

Examples from the RO authorities experience

Ministry of European Funds

Romania already has in place legal framework concerning the protection of whistle-blowers (Law 571/2004). By Order of the Minister of European Funds no. 353/2019 was approved the system procedure for reporting irregularities and the protection of the persons who complain or notice irregularities.

Ministry of Justice

The protection of the persons reporting on breaches of Union law is included among the preventive measures listed in Annex 3 to the National Anticorruption Strategy (NAS) regarding the inventory of measures of institutional transparency and prevention of corruption, as well as of the evaluation indicators,

NAS is focusing its efforts on strengthening integrity, reducing vulnerabilities and risks of corruption in the sectors identified as vulnerable to the phenomenon of corruption.

In order to achieve this objective, a knowledge of the situation on the ground is required, which is why monitoring the implementation of the strategy is carried out through a set of tools designed to facilitate the dialogue between all the participants in the fight against corruption and to allow: identifying the progress made in the NAS implementation; identifying and correcting the practical problems arising in the application of anti-corruption policies and norms; increasing the degree of knowledge, understanding and implementation of measures to prevent corruption.

One of these tools is the thematic evaluation missions. The evaluation procedure consists of completing the thematic evaluation questionnaire sent in advance to the evaluated public institution, organising the evaluation visit at its headquarters and drafting the evaluation report including good practices and recommendations.

In 2019 a number of 90 thematic missions for the evaluation of the 2016-2020 NAS implementation were carried out, at the level of the local public administration. These were organised in collaboration with the Ministry of Public Works, Development and Administration, based on the collaboration agreement concluded in 2016.

Among the topics that have been the subject of the evaluation missions mentioned above are the protection of the persons warning on integrity in the public interest.

Also, one of the objectives set in the NAS, relevant from the perspective of the protection of the integrity warning, is to increase the efficiency of the anti-corruption preventive measures by remedying the gaps and legislative inconsistencies regarding the ethics counselor, the protection of the warning in the public interest and the post-employment prohibitions (pantouflage).

The Ministry of Justice has endorsed the EU legislation on the protection of persons reporting violations of EU law, participating both through experts seconded within the RPRO BXL, as well as through experts from the Crime Prevention Directorate, in the negotiations regarding the Directive on the protection of persons reporting on breaches of Union law. This instrument was finalised during the PRES RO mandate, and its file constituted a priority.

On April 16, 2019, the European Parliament adopted the Directive at first reading, and subsequently, as mentioned above, on October 7, it was adopted by the Council of Ministers (JHA).

Managing Authority for Operational Programme Administrative Capacity

AM POCA had as source of detection of irregularities / frauds whistle-blowers or mass media reports, which, at the current date, are treated as being in the suspicion phase and undergo specialised checks / investigations.

Managing Authority for Regional Operational Programme

All the allegations of irregularity / fraud received through the whistle blowing system were transmitted for verification and investigated by the control structure within the Ministry of Public Works, Development and Administration and the confidentiality of the information regarding the identification data of the persons who transmitted the notification was ensured. These allegations, usually, have not been confirmed.

General Directorate for European Territorial Cooperation – Ministry of European Funds

All the allegations of irregularity / fraud received through the whistle blowing system were transmitted for verification and investigated by the control structure within the Ministry of Public Works, Development and Administration and the confidentiality of the information regarding the identification data of the persons who transmitted the notification was ensured. These allegations, usually, have not been confirmed.

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?☒YES, fully implementing the recommendation**.** Examples from the RO authorities experience: Ministry of European Funds Please see answer to Q 2.2.b.

Cooperation with judicial and administrative authorities is governed by national legislation and internal working procedures.

Managing Authority for Regional Operational Programme

There are requests for information and documents from the National Anticorruption Directorate, to which the Ministry of Public Works, Development and Administration responds promptly, but also requests formulated by the MPWDA to the NAD regarding the state of the NAD investigations. The information is requested for the correct updating and reporting of cases of suspected fraud. There is no collaboration protocol concluded between MPWDA and NAD, but there are two collaboration protocols concluded between MPWDA and The Fight Against Fraud Department and the National Agency for Integrity, respectively, regarding the exchange of information.

General Directorate for European Territorial Cooperation – Ministry of European Funds

There are requests for information and documents from the National Anticorruption Directorate, to which the Ministry of Public Works, Development and Administration responds promptly. Also, MPWDA requests DNA information on the status of investigations in order to update suspicion cases.

There is no collaboration protocol concluded between MPWDA and NAD, but there are two collaboration protocols concluded between MPWDA and The Fight Against Fraud Department and the National Agency for Integrity, respectively, regarding the exchange of information.

SI	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒NO *The MA (Government Office of the Republic SLOVENIA for Development and European Cohesion Policy) has in 2016 prepared a sectoral AFS that relates to the scope of the ECP for Objective 1* **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?**☒YES, partly implementing the recommendation *Government Office of the Republic SLOVENIA for Development and European Cohesion Policy answer: ARACHNE is mainly used by MA. ARACHNE is not always the best tool for the Slovenian situation (ARACHNE is very useful tool when we are dealing with non-Slovenian provider). Therefore, we use the information provided in different national computer applications that are publicly available (for example as provided by the Commission for the Prevention of Corruption called Erar, application Gwin, application e-credit) which provides date for additional verification options (appropriate for Slovenia*). *MA use risk analysis also for selection of the projects to be checked (by MA and IB) on the spot.* *This refers to risk analysis tools for the targeting of projects/operations to be submitted to specific verifications, on-the-spot checks, audits or other types of controls (as relevant). Please provide results in terms of irregularities/fraud detected during controls that have been started (also) because of risk analysis. The Irregularities Management System (IMS) provides this information, but the Member State may want to add detections that are excluded from reporting (such as detections before inclusion of expenditure in a statement of expenditure submitted to the Commission). The Member States are encouraged to provide relevant details to explain the actions undertaken or planned (in case of partial implementation) (see also question under section 2). If applicable, explain why no such action was taken.* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?**☒YES *Government Office of the Republic SLOVENIA for Development and European Cohesion Policy answer: Cooperation with the State Attorney's Office, better information with the IB, better cooperation with IB, early detection of fraud upon improved check lists, improved system performance and consequently fewer corrections.* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?**☒YES, partly implementing the recommendation *Government Office of the Republic SLOVENIA for Development and European Cohesion Policy answer: Cooperation with the Attorney-General and police will be strengthened. There is still room for improvements. Arachne was introduced and it is used mainly by MA. Arachne will be more spread to implement in future. More exchange of views and experiences with IB and AA on the matter.* **Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?**☒YES, partly implementing the recommendation

Government Office of the Republic SLOVENIA for Development and European Cohesion Policy answer: Guidance is in the process of setting out the procedure for lobbying. Whistle-blower norms will also be included in this guidance. In the case of consent, the guidance will be published on the MA website and thus binding for all IM Bodies. AAMRD-Agency for Agricultural Markets and Rural Developm.of the R. Slovenia answer: We encourage the employees to report any irregularities related to the Agency's scope of work. We have put a mailbox in the hallway for the employees to anonymously report irregularities or other infringements related to the funding or the administrative procedure. The applicants (or other parties, the public) on the other hand can choose a contact in the Agency's webside and report irregularities via e-mail.

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?☒YES, fully implementing the recommendation

Government Office of the Republic SLOVENIA for Development and European Cohesion Policy answer: We had an annual meeting with the DODV - State Attorney's Office at the end of 2019 to discuss outstanding issues and how the cooperation between the two bodies could be strengthened. The idea of connecting the State Attorney's Office with the State Prosecutor's Office dropped and the cooperation in the field of criminal law was dropped. The cooperation was found to be exemplary and positive for both sides. The result is also a table of all open procedures/cases where ECP is the subject/legal basis, as well as sending a few examples of open cases with brief descriptions of what stage / status they are in.

SK	*The Government Office of the Slovak republic, Central Contact Point for OLAF (CCP OLAF) as Slovak AFCOS contacted AFCOS network partners (national authorities, including managing authorities, certifying authority, control bodies and judicial authorities) in order to provide relevant information concerning the expenditure side of this material. AFCOS network partners provided information with respect to the questions in Risk analysis and Horizontal issues parts. CCP OLAF, the body who took part in preparing the Slovak National Anti-Fraud Strategy in cooperation with AFCOS network partners answered the questions relating to the National anti-fraud strategies.* **Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?** ☒*YES, fully implementing the recommendation* *The National Strategy for the Protection of the European Union's Financial Interests in the Slovak Republic (adopted in 2015), was updated in June 2019 in order to address new challenges in the area of the protection of the EU's financial interests. The updated version of The National Strategy for the Protection of the European Union's Financial Interests in the Slovak Republic (hereinafter referred to as "The Slovak NAFS") was approved by the Steering Committee for the Protection of the EU's Financial Interests in the Slovak Republic on 30 May 2019 and, subsequently signed by the Head of the Government Office of the Slovak Republic on 4 June 2019. The major novelty the updated version of The Slovak NAFS introduces are the new tasks for years 2019 – 2020 defined in the Action Plan, which forms one of The Slovak NAFS annex. In addition, some of the tasks from the previous Action Plan have been moved to the main text of The Slovak NAFS as permanent tasks. The updated version of The Slovak NAFS was send to OLAF in December 2019.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?**☒YES, fully implementing the recommendation *The Slovak NAFS, updated in 2019, was approved by the Steering Committee for the Protection of the EU's Financial Interests in the Slovak Republic, in which 21 network partners are represented, including representatives from General Prosecutors Office of the Slovak Republic, National Criminal Agency and Ministry of Justice of the Slovak Republic. AFCOS network partners were engaged in commenting on the final version of The Slovak NAFS.* **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?**☒ YES, partly implementing the recommendation *The updated version of the Slovak NAFS has taken into account the need for improved coordination between administrative and judicial authorities. Regarding the new Action Plan (annex of the Slovak NAFS) the CCP OLAF in cooperation with other relevant authorities prepares an overview of the most frequent forms of fraud in the implementation of EU funds identified during the 2007-2013 and 2014-2020 programming periods and at the same time prepares an analysis of cases in which the AFCOS network partners identified suspicion of criminal offences harming the EU's financial interests in Slovakia in the course of the controls/audits/checks performed (statistics, number of cases, etc.). These two tasks will be developing in cooperation with representatives from Managing Authorities, General Prosecutors Office of the Slovak Republic, Ministry of Finance of the Slovak Republic, etc.*

Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations; ☒ YES, partly implementing the recommendation

The Slovak NAFS emphasises that "structured coordination (information and data exchange) between the anti-fraud authorities, managing authorities and other stakeholders represents a good practice. However, effective investigation of fraud cases requires establishing closer cooperation links between the bodies responsible for the implementation of EU funds on the one hand, and the law enforcement and judicial authorities on the other. Cooperation between the AFCOS network partners should focus on information exchange and operational assistance."

The Slovak NAFS and the Action Plan, which forms its annex, contain various tasks focused on improving the coordination between administrative and criminal authorities. One of these tasks, defined in the Action plan, is to set up a network of liaison officers at the level of the AFCOS network partners (these partners include also representatives from individual Managing Authorities, General Prosecutors Office of the Slovak Republic, National Criminal Agency of Slovakia, Ministry of Justice of the Slovak republic) to enhance the effectiveness of operational cooperation in the area of protection of EU's financial interests in Slovak republic. This task was completed in the end of 2019 and the Slovak AFCOS have started to use the network of liaison officers for purposes of coordination of the operational cooperation in the area of the protection of the EU´s financial interests.

In order to exchange good practice and information, the CCP OLAF, in cooperation with AFCOS network partners, also organises anti-fraud trainings focusing on the protection of the EU's financial interests. CCP OLAF currently organises training sessions in cooperation with experienced prosecutors and police investigators from GPO and National Crime Agency. The list of trainings for 2017-2018 shows that ten seminars took place covering a wide variety of topics on the protection of the EU's financial interests. Several repeated sessions were related to the following areas: awareness of fraud are collusion, cartels and distortion of competition, the most common infringements of public procurement rules, and detection of fraudulent practices in the implementation of ESI Funds.

Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?☒ NO

The assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests, as such, is not carried out, but every year, the Secretariat of the Steering Committee for the Protection of the EU's Financial Interests in the Slovak Republic, based on the information from the network partners, informs the Steering Committee about the fulfilment of the tasks defined in The Slovak NAFS and in The Action Plan, which forms one of the annexes of The Slovak NAFS.

Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?☒YES, fully implementing the recommendation

I. The Ministry of Environment of the Slovak Republic (fully implemented the recommendation) as the Managing Authority for the Operational Programme Quality of Environment (hereinafter "MA") uses

system ARACHNE as an auxiliary tool and source of information for evaluating individual risk indicators. MA carries out risk / fraud risk management relevant to the Operational Programme Quality of Environment.

II. The Ministry of Agriculture and Rural Development of the Slovak Republic (fully implemented the recommendation.) Managing authorities for the operational programmes use IT tools (such as ARACHNE, IT monitoring system ITMS2014+ etc.) and has also established risk management task forces for programmes in accordance with the European Commission Guidelines for Member States and Programme Managers on fraud risk assessment and effective and proportionate anti-fraud measures of 16 June 2014 (EGESIF_14-021-00-16 / 06/) to detect irregularities and fraud. Agricultural paying agency uses IT tools ARACHNE.

III. The Ministry of Education, Science, Research and Sport of the Slovak Republic fully implemented the recommendation. At the Ministry of Education, Science, Research and Sport of the Slovak Republic as the Intermediate Body for the Operational Programme Integrated Infrastructure (formerly the Managing Authority for the Operational Programme Research and Innovation) and as the Intermediate Body for the Human Resources Operational Programme was created by local administrator ARACHNE (LA ARACHNE). LA ARACHNE manages users' access to ARACHNE for the relevant operational programme. LA ARACHNE is managed by a manager of ITMS. The ARACHNE system and its use is described in Chapter 7 of the IT Monitoring System - ITMS2014 + in the Procedures Manual, which also includes the ARACHNE Risk Verification Checklist.

In 2019, The Ministry of Education, Science, Research and Sport of the Slovak Republic updated: Fraud Risk Catalog "Fraud Risk Assessment and Effective and Appropriate Measures Against Fraud", Comprehensive Risk Catalog, Risk Management Procedures and Statute and Rules of Procedure of Working Group for risk management.

The irregularities found so far have not resulted from checks carried out for risk analysis. The irregularities detected under OP II (formerly OP Research&Innovations) did not result from checks carried out for risk analysis. The irregularities recorded under OP II (formerly OP Research&Innovations) were identified on the basis of media coverage of calls for applications for a non-repayable financial contribution to support and irregularities resulting from the investigation of the National Criminal Agency (NCA).

Irregularity registered on the base of the letter from the NCA, by which the NCA asked the Ministry of Education, Science, Research and Sports of the Slovak Republic to provide cooperation in the investigation of suspected criminal the offence of damaging the European Union's financial interests. The case is being prosecuted (for the offence of damaging the financial interests of the European Union in parallel with the crime of machinations in public procurement and public auctions).

IV. The Ministry of Interior of the Slovak Republic also fully implemented the recommendation.

V. The Ministry of Finance, Audit Authority verifies the management and control system of managing authorities and others relevant authorities as a part of the system audit. Within the audit the risk analysis elaborated by the managing authority is checked also. When verifying the risk analysis, the audit authority verifies that the Managing Authority has implemented the recommendations and guidelines developed by the European Commission (including recommendations on usage of relevant IT tools).

VI. The Public Procurement Office partly implemented the recommendation. Since 1st April 2019, low value contracts can be awarded through the electronic public procurement system "EVO".

VII. The Antimonopoly Office of the Slovak Republic (also partly implemented the recommendation) ensured access to the ARACHNE system for the employees of the Office. At the request of the Office were organised additional training tailored to new functions of the ARACHNE, which will be relevant for the Office. Based on this training The Antimonopoly Office of the Slovak Republic plans to start to use the relevant functionalities of ARACHNE within the investigation activities.

VIII. The Supreme Audit Office of the Slovak Republic

According to the Constitution of the Slovak Republic, the Supreme Audit Office of the Slovak Republic is an independent body. Therefore, internal procedures, strategies and analysis are developed and applied independently, according to the relevant standards.

We consider coordination among the authorities concerned to be above standard, as the Supreme Audit Office of the Slovak Republic has some concluded cooperation memoranda.

SAO has an effective monitoring system in place based on information from the media.

Unfortunately, SAO has not been allowed access to ARACHNE. Nevertheless, the Supreme Audit Office of the Slovak republic collects the necessary information, data and documents for the purposes of risk analysis. This is done through its own monitoring and legal documents and/or information requests.

Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?☒YES

I. The Ministry of Interior of the Slovak Republic: (YES)

Finding 1.: Insufficient monitoring of the effectiveness of anti – fraud measures

Measures: The Managing Authority (MA) updated the Internal procedures documentation. The update concerns especially the performance monitoring of anti – fraud measures which will be carried out not just through the relevant indicators (which are compared also with other operational programmes) but also by the MA employees who are members of the Working group for risk management on the level of Department of European policies of the Ministry of Interior. The monitoring process is also ensured by the list of controls, audits and certifying verifications which are the basic framework for the MA for working out the Annual report on anti – fraud strategy.

Finding 2: Insufficient awareness of the anti – fraud prevention measures

Measure: The Managing authority has updated its Communication strategy, especially the part of anti – fraud prevention and detection.

II. The Ministry of Agriculture and Rural Development of the Slovak Republic (YES)

In line with the zero-tolerance approach to fraud, the Managing authority for the programmes Interreg SK-CZ and SK-AT prepared and published anti-fraud policy document. Managing authorities use a risk analysis to identify the most vulnerable areas of fraud. Managing authorities also use IT tools such as ARACHNE, IT monitoring system ITMS2014+ and whistleblowing system.

III. The Ministry of Environment of the Slovak Republic (YES)

MA for the Operational Programme Quality of Environment (hereinafter "OP QE") carries out the management of risks / risks of frauds relevant to the OP QE in accordance with EGESIF_14-0021-00 of 16 June 2014 "Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures" and in line with the Risk Management Procedures of the OP QE.

IV. As the fraud risk assessments and setting the procedures which reflects the existing risks are prior responsibilities of the other authorities (e.g. managing authority), The Ministry of Finance of the Slovak Republic as the Audit Authority and The Public Procurement Office do not share any results in this field. The audit authority performs audits (system audit and audit of operation).

2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure? ☒YES, partly implementing the recommendation

I. The Ministry of Agriculture and Rural Development of the Slovak Republic and The Agricultural Paying Agency (YES, partly implementing the recommendation)

The Agricultural paying agency shall carry out on-the-spot checks to determine the origin of the property.

II. The Ministry of Interior of the Slovak Republic: (Yes, partly implementing the recommendation

Finding: Identified insufficient strategy for improving professional skills in the area of anti – fraud prevention and detection

Implemented measures

Two employees of the Department have been designated to participate in training concerning the anti – fraud prevention and detection, organised by the European Commission and Office of Government.

Measures to be implemented: The MA has sent the request to the Central Coordination Body (CCB), which is responsible for education and trainings for employees who are implementing the EU funds, to complete the education plan by the activities concerning the issue of anti – fraud prevention and detection. In case of positive feedback from the CCB, the Managing authority will nominate all the employees who are members of the Working group for risk management, to participate in this kind of activities.

III. The Ministry of Finance of the Slovak Republic as the Audit Authority

The audit authority performs audits (system audit and audit of operation). The fraud risk assessments and setting the procedures which reflects the existing risks are prior responsibilities of the other authorities (e.g. managing authority).

IV. The Public Procurement Office (No)

Risk analysis is in competence of Managing Authorities.

Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism? ☒YES, fully implementing the recommendation

In 30 January 2019, Slovakia adopted Act no. 54/2019 Coll. Act on the protection of whistleblowers of anti-

social activity and on amendments to certain acts. This new Act strengthens the position of whistleblowers and indirectly help to protect of the EU financial interests and make the fight against fraud more effective. The act is effective as of 26 February 2019. The subject of this act are conditions for provision of protection of persons against unjustified punishment in the employment relationship in connection with the reporting of crime or other anti-social activity as well as the rights and obligations of natural persons and legal persons in the reporting of anti-social activity. This legislative also creates in Slovakia a new Office for the Protection of Whistleblowers, with new competencies in this field, because as an independent state administration body can provide the protection of whistleblowers more effective, and could effectively help with the fight against the fraud.

I. The Ministry of Culture of the Slovak Republic (YES, fully implementing the recommendation.)

Ministry of Culture of the Slovak Republic prepared the Anti-Corruption Programme 2019 (document has been approved in August 2019), on the basis of the Government Resolution no. 585/2018 of 12 December 2018, named the Anti-Corruption Policy of the Slovak Republic for the years 2019 – 2023.The anti-corruption programme has been developed to improve the anti-corruption preventing and combating corruption by identifying corruption risks and causes corruption to prevent the emergence of new conditions, opportunities and situations for corrupt behaviour in the resort.

II. The Ministry of Agriculture and Rural Development of the Slovak Republic and The Agricultural Paying Agency (YES, fully implementing the recommendation.)Information and instructions for spontaneous reporting of potential irregularities are published on the websites of the Ministry of Agriculture and Rural Development of the Slovak republic and Agricultural Paying Agency. The Organisation has set up emails to facilitate reporting fraud.

Organisations has created a whistleblowing system and communicate all suspicions of fraud to criminal investigation or prosecution bodies and also if it is needed cooperate with any others, such as OLAF. The protection of whistle-blowers is carried out under the new Whistleblower Protection Act (Act. No. 54/2019 Coll. SK).

III. The Ministry of Education, Science, Research and Sport of the Slovak Republic (YES, fully implementing the recommendation)

In 2019, the Ministry of Education, Science, Research and Sport of the Slovak Republic, as an intermediary body for OP II (formerly OP VaI), issued the document Anti-fraud Policy. The aim of this policy is to promote a culture to discourage people from committing fraud and to facilitate the prevention and detection of fraud. The document contains procedures to assist in the investigation of fraud and related crimes and to ensure that fraud will solved in a time and appropriate and responsible manner. The document identifies options for anonymous and non-anonymous reporting of fraud.

IV. The Ministry of Environment of the Slovak Republic (fully implemented the recommendation)

The management documentation for the OP QE includes the implementation of the fraud notification system, the key element of which is the protection of whistle-blowers in accordance with the above mentioned Act.

Currently, in relation with the OP QE it is possible:

- Anonymous or non-anonymous reporting of potential risks, including suspicion of fraud and illegal activities at the email address: rizika_opkzp@enviro.gov.sk, - Anonymous corruption reporting via a telephone line established by the MoE SR in the framework of the transparency policy: https://www.minzp.sk/strazca/, - Anonymous or non-anonymous corruption reporting via the telephone line established by the Office of the Government of the Slovak Republic, available at: www.bojprotikorupcii.vlada.gov.sk,

- Non-anonymous reporting of suspected criminal offences or other illegal activities, with an impact on EU and Slovak Republic finances on the e-mail address: infoirq@minv.sk established by the National Criminal Agency of the Presidium of the Police Force, - Anonymous reporting of suspected fraud and irregularities with an impact on EU funds to the European Anti-Fraud Office (OLAF EC): https://fns.olaf.europa.eu/.

V. The Public Procurement Office (YES, partly implementing the recommendation)

To report suspected irregularities in public procurement, the Public Procurement Office has set up the following e-mail address: irregularities@uvo.gov.sk.

VI. The Ministry of Finance (Audit Authority):

Potential irregularities are reported different ways. The audit authority deals with all the reports (even anonymous ones).

VII. The Antimonopoly Office of the Slovak Republic

The protection of whistle-blowers in the area of the competence of the Antimonopoly Office of the Slovak Republic is laid down in the relevant provisions of § 38 of the Law on the Protection of Competition No 136/2001 Coll. as amended (the reward for the submission of the evidence on the existence of agreements restricting competition) and also in the Guidance Note on selected issues of the procedure of the Antimonopoly Office of the Slovak Republic, where evidence of an agreement restricting competition is submitted.

Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?☒YES, fully implementing the recommendation

In the area of trainings the CCP OLAF has organised training activities and seminars for AFCOS network partners based on the Training Plan for the Protection of the EU's Financial Interests in the Slovak Republic. The list of trainings for 2017-2018 shows that ten seminars took place covering a wide variety of topics on the protection of the EU's financial interests. Several repeated sessions were related to the following areas: awareness of fraud are collusion, cartels and distortion of competition, the most common infringements of public procurement rules, and detection of fraudulent practices in the implementation of ESI Funds.

I. The Ministry of Finance of the SR, Certifying authority (CA)

(YES, fully implemented the recommendation)

Taking into account that there have not been adopted any new laws or national measures regulating the co-operation between the Certifying Authority (CA) and the judicial and administrative authorities in the Slovak Republic, no significant changes compared to 2018 took place. It is, therefore, valid that we always

promote the cooperation between judicial and administrative authorities. The Certifying Authority considers close cooperation with above mentioned authorities as essential, especially in relation to Managing Authorities. CA does not have a necessity to cooperate with mentioned authorities on a regular basis, since all the data related to CA work are obtained through Managing Authorities. However, CA itself had taken steps to strengthen relationship with the Public Procurement Office and the Antimonopoly Office by closing memorandum of cooperation. CA works on closing of a co-operation agreement with the Supreme Audit Office. As to the judicial authorities, CA agenda does not require direct cooperation, nevertheless CA is regularly analysing the decisions issued by courts. When CA is approached by administrative authorities, a court or law enforcement authorities with the request for co-operation, CA always provides all available information in order to contribute to clarifying respective matters at the earliest possible date. The obligation to cooperate closely and exchange all necessary information between authorities directly results from several specific regulations.

II. The Ministry of Education, Science, Research and Sport of the Slovak Republic (YES, fully implemented the recommendation)

As an example, one of the irregularities was registered on the base of the letter from the National Criminal Agency (NCA) by which the NCA asked the Ministry of Education, Science, Research and Sports of the Slovak republic to submit documentation for an ongoing investigation into the criminal offence of Machinations in public procurement and public auction in conjunction with the crime Damaging the European Communities' financial interests.

III. The Public Procurement Office

(YES, fully implemented the recommendation)

In 2018, the Chairman of the Public Procurement Office started to deepen cooperation in the control of public procurement with key central state administration and judicial bodies on the basis of signed cooperation agreements. Those are:

• Antimonopoly Office of the SR,

• Supreme Audit Office of the Slovak Republic,

• General Prosecutor's Office of the Slovak Republic,

• Ministry of Finance of the Slovak Republic as the Audit Authority

IV. The Ministry of Environment of the Slovak Republic

(YES, partly implemented the recommendation)

The MA for the OP QE carries out regular quarterly monitoring of all ongoing judicial proceedings in which the Ministry of Environment of the Slovak republic acts as a party (or injured party) and which resulted from the implementation of the OP QE. At the same time, the MA provides all the cooperation necessary for the detection of irregularities, incl. fraud, in relation to both courts and law enforcement agencies. We would like to point out the fact that in line with the Manual of Procedures of the MA for the OP QE, the MA employees are obliged to report suspicion of committing a crime to relevant units of the Police Force.

FI	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?**☒NO *At this stage a separate national anti-fraud strategy is not deemed to be a priority as the national administration is working with other strategies related to issues in the same field such as anti-corruption and shadow economy.* **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?**☒YES, partly implementing the recommendation *Risk analysis for expenditure from EAGF and EAFRD is updated annually or when needed. The updated information is taken into the actual guidance notes and checklists for administrative controls, which are built into the respective IT-systems. In ERDF and ESF, training is provided for the intermediate bodies of different types of fraud cases.* **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?**☒NO *So far, the findings brought forward have mostly been acknowledged in the risk analysis.* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?**☒YES, partly implementing the recommendation *In EAGF and EAFRD, a separate risk analysis has been carried out for different types of measures.* **Q.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?**☒YES, partly implementing the recommendation *Possibility for anonymous reporting was established for structural funds.* **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?** ☒NO

SE	**Q.2.1. Have you adopted or updated a national anti-fraud strategy, which you have communicated to the European Commission/OLAF?** ☒NO *Answer: All Swedish authorities managing EU funds have individual anti-fraud strategies. Essential sections are shared by the authorities while other sections are individually drafted, since some authorities have broader areas of responsibility than that of managing EU funds. To compile these strategies into one serves no purpose.* **Q.2.1.a. If yes, have you developed this strategy in cooperation with all bodies and authorities which have a specific role and expertise in the protection of the EU financial interests, including law enforcement and prosecution services?**☒YES, partly implementing the recommendation *Answer: Essential sections of the strategy like the policy of compulsory reporting to the prosecution authority and instructions regarding how to handle suspected fraud have been jointly developed within the Council for the Protection of EU´s Financial Interests in Sweden (the SEFI-council) chaired by the Swedish Economic Crime Authority. Other sections are individually developed.* **Q.2.1.b. In line with what had been recommended in previous years, has your national anti-fraud strategy taken into account the risk analysis conclusions contained in the 2018, 2017 and 2016 PIF reports?** X YES, partly implementing the recommendation *Answer: The PIF reports like other recommendations from the Commission are considered along with other data when the authorities revise their strategies, which is done annually.* **Q.2.1.c. In line with what was recommended in previous years, has your national anti-fraud strategy taken into account the need to structure the coordination between administrative and criminal checks and investigations;** X YES, partly implementing the recommendation *Answer: Sweden regards this as one of the most important issues to work with. Formally all concerned parties make the correct distinctions in their strategies, policies, guidelines etc. However, the formal distinction seems not to have an impact on the number of reported suspected fraud to the Prosecution authority. That is why the SEFI-Council in accordance with a statement made by the management of all concerned authorities in December 2019 decided to make a study very much like ECA´s report 06/2019 in order to learn whether the staff of the authorities fail to report suspected fraud when they identify irregularities.* **Q.2.1.d. Did you make any assessment of the impact of the NAFS on the fight against fraud affecting the EU's financial interests?** NO **Q.2.2.a. In line with what was recommended in previous years, has risk analysis been strengthened to detect irregularities and fraud, including the use of IT tools (such as ARACHNE)?**☒YES, partly implementing the recommendation Answer: The risk analysis work carried out by the concerned authorities are continuously focusing on

	enhancing the strategies used. The larger Swedish authorities have special risk assessment teams for this assignment and in this context the SEFI-council serves as a fora for exchange of best practices and facilitates educational seminars and so on. How the authorities deal with risk analysis is also monitored according to the Swedish regulation (2007:603) of internal risk and control. **Q.2.2.b Can you share any results deriving from the use of the findings from PIF Reports in your fraud risk assessments?**☒NO *Answer: Typically, the results of the PIF report are not direct applicable to the Swedish conditions. Therefore, it is more correct to say that the findings of the PIF report may inspire Swedish authorities to consider a finding but in a Swedish environment. One such subject – area of concern - is public procurement.* **Q.2.2.c Have you further exploited the potential of risk analysis, tailoring the approach to the different types of expenditure?**☒YES, partly implementing the recommendation *Answer: The annual assessment and continuous revision performed by the risk assessment teams of the authorities are carried out with the purpose of identifying new risks, evaluating actions taken etc. in order to formulate an action plan for dealing with risks the following year. Typically, the Swedish authorities who manages EU funds only deal with one type of expenditure rather than several different types of expenditure.* Q**.2.3.a Have you facilitated and assessed the spontaneous reporting of potential irregularities and strengthen the protection of whistle-blowers, who are also a crucial source for investigative journalism?**☒YES, fully implementing the recommendation *Answer: Several authorities have a whistle-blower function in place and policies to strengthen the protection of whistle-blowers. One of the largest newspapers (Dagens nyheter) have written several articles about some suspected irregularities in the Swedish ESF Council. The newspaper have gotten access to all documents thanks to the Swedish Public Access to Information and Secrecy Act.* **Q.2.3.b Have you promoted systematic and timely cooperation between judicial and administrative authorities?**☒YES, fully implementing the recommendation *Answer: The eight managing authorities (some are administrative and some judicial) have regular networking meetings several times a year. They meet to discuss the implementation of EU programmes, take part in COCOLAF meetings and are also part of the SEFI Council which is headed by the Swedish Economic Crime Agency.*