Preventing fraud and corruption in the European Structural and Investment Funds – taking stock of practices in the EU Member States

Compendium of anti-fraud practices for preventing and detecting fraud and corruption in ESI Funds

Written by *Léna Bonnemains, Melissa Campagno,*
Brian Kessler, Olga Mala, and Goya Razavi
5 October 2018

DISCLAIMER

The authors of this document are Léna Bonnemains, Melissa Campagno, Brian Kessler, Olga Mala, and Goya Razavi. The information and views set out in it are those of the authors and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in it. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

EUROPEAN COMMISSION

Directorate-General for Regional and Urban Policy
Directorate E - Administrative Capacity Building and Programmes Implementation II
Unit REGIO.DDG.E.1

Contact: Inguna Kramina

E-mail: *REGIO-E1-ADMINISTRATIVE-CAPACITY@ec.europa.e*

European Commission
B-1049 Brussels

EUROPEAN COMMISSION

Preventing fraud and corruption in the European Structural and Investment Funds – taking stock of practices in the EU Member States

Compendium of anti-fraud practices for preventing and detecting fraud and corruption in ESI Funds

Directorate-General for Regional and Urban Policy

2019 EN

Manuscript completed in October 2018

The European Commission is not liable for any consequence stemming from the reuse of this publication.

Luxembourg: Publications Office of the European Union, 2019

ISBN 978-92-76-08799-1
doi: 10.2776/488340

Table of Contents

1. Introduction

With approximately EUR 460 billion allocated for the 2014-2020 programming period, the European Structural and Investment (ESI) Funds (consisting of the Cohesion Fund (CF), the European Regional Development Fund (ERDF), the European Social Fund (ESF), the European Agricultural Fund for Rural Development (EAFRD), and the European Maritime and Fisheries Fund (EMFF)) represent almost a third of the EU budget.

ESI Funds finance operational programmes (OPs) in Member States (MS), each aimed at achieving specific objectives within the areas defined as EU priorities. About 400 OPs are funded through ESI Funds for the 2014-2020 programming period and managed by competent authorities within each EU Member States.

The European Commission (EC) and MS share responsibilities for the implementation and management of ESI Funds, and both must ensure funds are spent properly and achieve the greatest possible impact. Moreover, they must put in place the proper safeguards to limit the risks of fraud and corruption. Fraud is defined by the Convention on the protection of the European Communities' financial interests as the deliberate act of deception intended for personal gain or to cause a loss to another party. A definition of corruption used by the EC is the abuse of (public) position for private gain. Example of fraudulent and corrupt practices can include but are not limited to conflict of interest, double funding, bribery or falsification of document.

Authorities in the MS have the legal obligation to safeguard EU funds as per Article 325 of the Treaty on the Functioning of the European Union and Article 59(2) of the Financial Regulation. This obligation was specified and reinforced in 2013 by Article 125(4)(c) of the Common Provisions Regulation (CPR). Article 125(4)(c) requires the implementation of risk-based, effective and proportionate measures to prevent fraud in managing and controlling the OPs.

2. Objective of this Compendium

The purpose of this Compendium is to present a sample of anti-fraud practices identified in the context of the study on preventing fraud and corruption in ESI Funds. This study aims at taking stock of and disseminating information on anti-fraud measures put in place by authorities responsible for the management and control of ESI Funds in the 28 EU MS to prevent and detect fraud and corruption.

Anti-fraud practices featured in this Compendium consist of relevant measures developed by ESI Funds practitioners at the regional, national and EU level, which represent strong potential candidates for good practices in the fight against fraud and corruption. This Compendium also informs about other measures developed by non-ESI Funds practitioners that bring a positive a positive impact to the MS' anti-fraud system.

The Compendium targets ESI Funds management practitioners and policy makers who are exploring ways to improve their national management and control system or elements of it.

3. Glossary of key concepts

European Structural and Investment (ESI) Funds

ESI Funds includes the Cohesion Fund (CF), the European Regional Development Fund (ERDF), the European Social Fund (ESF), the European Agricultural Fund for Rural Development (EAFRD), and the European Maritime and Fisheries Fund (EMFF).

European Anti-Fraud Office (OLAF)

OLAF investigates fraud against the EU budget, corruption and serious misconduct within the European institutions, and develops anti-fraud policy for the EC.

Fraud

Fraud is defined by the Convention on the protection of the European Communities' financial interests as the deliberate act of deception intended for personal gain or to cause a loss to another party.

Corruption

A definition of corruption used by the European Commission (EC) is the abuse of (public) position for private gain.

Practice

For the purposes of this compendium, we considered as "practice" a solution or approach implemented by one or several authorities within the EU Member States (MS) that deserves special attention because of its potential to improve anti-fraud and anti-corruption systems.

Operational Programmes (OPs)

ESI Funds are used to finance several Operational Programmes (OPs), each aiming at achieving specific objectives within the areas defined as EU priorities. ESI Funds' competent authorities within the EU MS are responsible for the sound management and control of OPs.

Managing Authorities (MAs)

MAs are responsible for managing one or several OPs in accordance with the principle of sound financial management. The MA is also the end-responsible for putting effective and proportionate anti-fraud measures in place on risk-based approach.

Common Provision Regulation (CPR)

Regulation (EU) N1303/2013 of the European Parliament and of the Council of 17 December 2013 laying down common provisions on the ERDF, the CF, the EARDF and the EMFF, and laying down general provisions on the ERDF, the ESF, the CF and the EMFF funds and repealing Council Regulation (EC) No 1083/2006.

Audit Authorities (AAs)

AAs ensure that audits are carried out on the proper functioning of the Management and Control System (MCS) of the OP. As a part of the assurance that the AAs give, they have the obligation to verify and monitor how the MA complies with Art. 125(4)(c) of the CPR. Auditors have a key role (both an audit and an advisory role) in providing an opinion on the functioning of management and internal control systems for OP that are part of the ESI Funds. They have an obligation in the fight against fraud and must assist the MS in preventing, detecting and correcting irregularities and fraud.

Certifying Authorities (CAs)

CAs are responsible for, amongst others, drawing up and submitting payment applications to the Commission, and certifying that they result from reliable accounting systems, are based on verifiable supporting documents, and have been subject to verifications by the MA. Additionally, they are responsible for certifying the completeness, accuracy and veracity of the accounts and that the expenditure entered in the accounts complies with applicable law.

Anti-Fraud Coordination Service (AFCOS)

The OLAF Regulation has created the requirement for MS to designate a service ('the anti-fraud coordination service') to facilitate effective cooperation and exchange of information, including information of an operational nature, with OLAF (Article 3 (4) of the OLAF Regulation). Following this requirement to establish an AFCOS, the Commission has issued a Guidance Note on the main tasks and responsibilities of an AFCOS. It has to be kept in mind that in each country, AFCOS set-up, role and functions differ in many ways.

Intermediate Bodies (IBs)

MAs and CAs may also delegate some of their duties to Intermediate Bodies (IBs). An IB is any public or private body, which acts under the responsibility or carries out duties on behalf of an MA (or sometimes a CA).

Beneficiaries

Beneficiaries are the (public or private) bodies that receive financing from the MA or IBs. They are responsible for executing the projects for which the financing has been received.

Red flags

Red flags can be defined as a set of indicators that may signal possible fraud. Red flags do not indicate fraud by themselves but provide possible warning signs of fraud.

4. Approach

A good practice is commonly understood as a solution or approach that can be assessed as having a positive verified impact on a specific issue. However, when it comes to the fight against fraud and corruption, establishing a clear link between the effects of a practice implemented and the reduction of fraud and corruption is not straightforward as evidence of the impact on fraud and corruption of any measure is particularly difficult to gather. For instance, a reduction of fraud cases detected does not necessarily mean that fraud has decreased, but can also mean that the system is less efficient in detecting fraud.

Furthermore, as a large part of the anti-fraud practices featured in this Compendium have been implemented in response to the new requirements brought by the 2014-2020 programming period, it is too soon at this stage to call those practices **good** practices. Indeed, authorities who have implemented them have not yet collected sufficient insights to assess the results of the practice on their anti-fraud system. Therefore, this Compendium focus on examples of identified anti-fraud practices, which display a strong potential to be considered good practices at a time when, and if, their impact on fraud and corruption can be assessed.

Anti-fraud practices presented in this Compendium were primarily identified when discussing with MAs, AAs, AFCOS, and CAs where relevant, during more than 140 interviews conducted. Interviews were complemented by desk research work and insights collected from speakers who presented their anti-fraud practice on this occasion of the 13 September workshop on preventing fraud and corruption in ESI Funds.

An initial list of 104 practices examples were identified and further refined to obtain a sample of 65 practice examples. In order to select the best examples from this sample and to feature them in this Compendium, we relied on opinions of stakeholders interviewed, and on PwC experts' qualitative assessment based on the following two criteria:

1. **Potential impact:** whether the practice has the potential to positively impact the anti-fraud system of the MS;
2. **Transferability and applicability:** whether the practice is seen as easily transferable and applicable to other contexts (e.g. other OPs or MS). This criterion ensures that the selected anti-fraud practices are relevant for a maximum of OPs and MS.

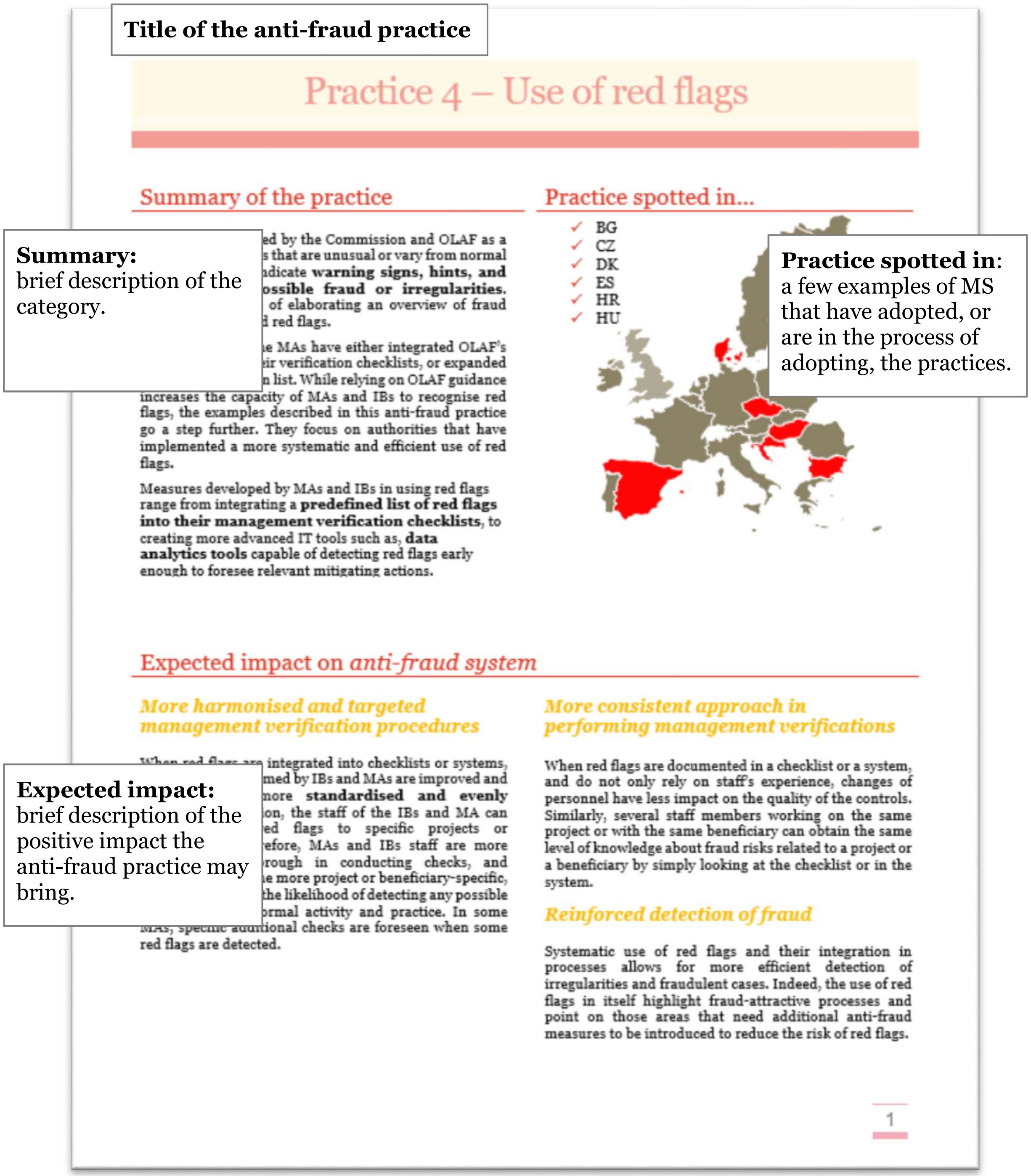
In very few cases, and for the reasons abovementioned, the **innovative and unique character** of the anti-fraud practice was considered i.e. whether the practice display innovative characteristics that differentiate it from what is usually done.

As a result, this Compendium encompasses two types of anti-fraud practices. For the main part, practice examples presented consist of good implementations of suggestions, guidelines, and requirements of the EC (e.g. designation criteria). For a small part, practice examples highlight unique and innovative features of certain examples. These were usually put in place on the sole initiative of practitioners or authorities, or as part of other initiatives.

Following this assessment, we grouped the shortlisted practice examples into 8 categories of practices featuring 25 examples and case studies. Hence, a fiche in the Compendium corresponds to a category of anti-fraud practices, e.g. "Practical anti-fraud trainings". The anti-fraud practice fiches further include descriptions of some of the identified examples in order to illustrate the various practical ways to implement the anti-fraud practice.

5. How to use this Compendium

Each anti-fraud practice is described in a “fiche”. Each fiche is composed of 3 to 8 pages. The content of the first page of the fiches is described below.



Title of the anti-fraud practice

Practice 4 – Use of red flags

Summary of the practice

Summary: brief description of the category.

ed by the Commission and OLAF as a
s that are unusual or vary from normal
ndicate **warning signs, hints, and**
ossible fraud or irregularities.
of elaborating an overview of fraud
d red flags.

e MAs have either integrated OLAF's
eir verification checklists, or expanded
n list. While relying on OLAF guidance increases the capacity of MAs and IBs to recognise red flags, the examples described in this anti-fraud practice go a step further. They focus on authorities that have implemented a more systematic and efficient use of red flags.

Measures developed by MAs and IBs in using red flags range from integrating a **predefined list of red flags into their management verification checklists**, to creating more advanced IT tools such as, **data analytics tools** capable of detecting red flags early enough to foresee relevant mitigating actions.

Practice spotted in…

- ✓ BG
- ✓ CZ
- ✓ DK
- ✓ ES
- ✓ HR
- ✓ HU

Practice spotted in: a few examples of MS that have adopted, or are in the process of adopting, the practices.

Expected impact on *anti-fraud system*

More harmonised and targeted management verification procedures

Expected impact: brief description of the positive impact the anti-fraud practice may bring.

When red flags are integrated into checklists or systems,
med by IBs and MAs are improved and
more **standardised and evenly**
on, the staff of the IBs and MA can
ed flags to specific projects or
efore, MAs and IBs staff are more
rough in conducting checks, and
e more project or beneficiary-specific,
the likelihood of detecting any possible
ormal activity and practice. In some
MAs, specific additional checks are foreseen when some red flags are detected.

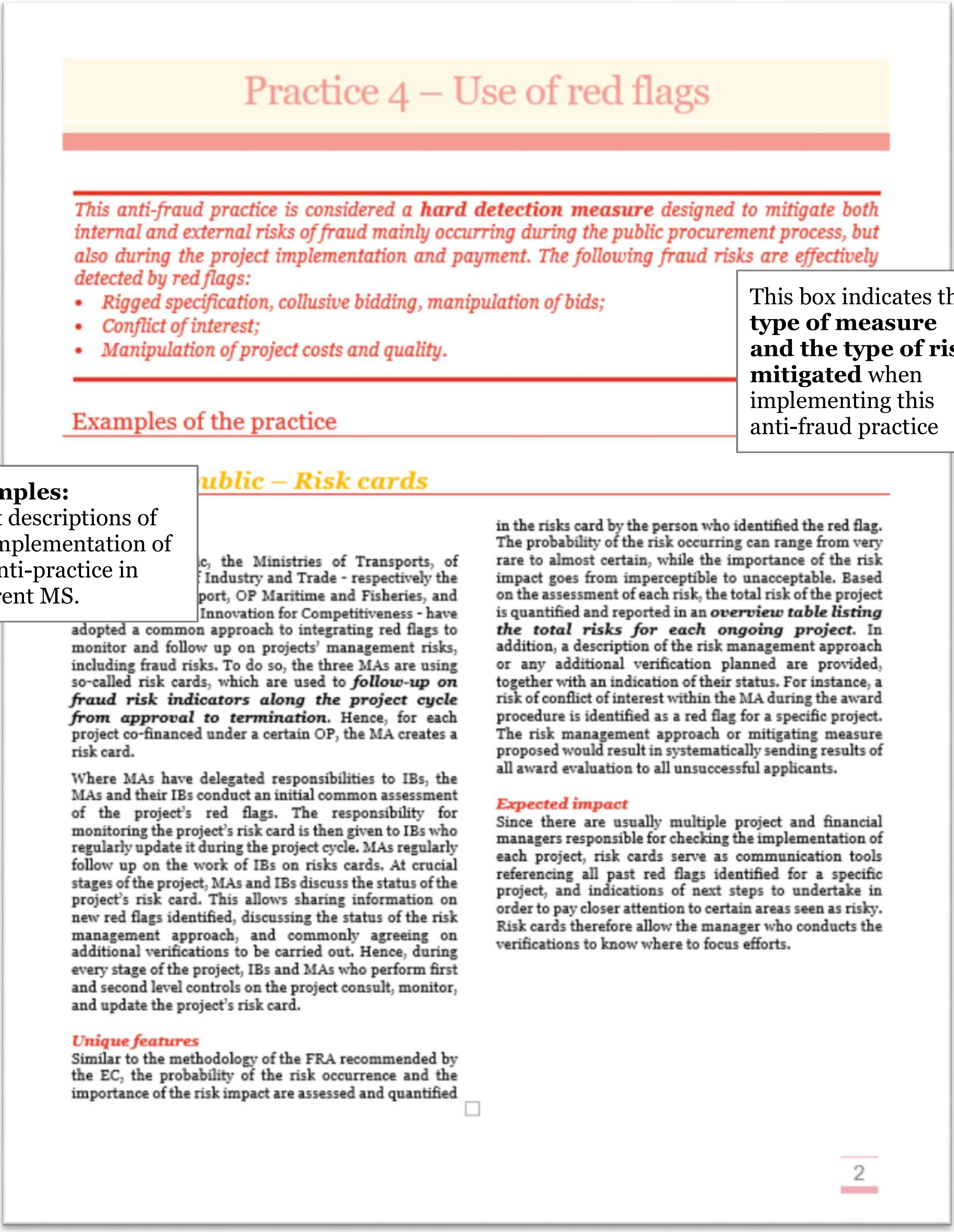
More consistent approach in performing management verifications

When red flags are documented in a checklist or a system, and do not only rely on staff's experience, changes of personnel have less impact on the quality of the controls. Similarly, several staff members working on the same project or with the same beneficiary can obtain the same level of knowledge about fraud risks related to a project or a beneficiary by simply looking at the checklist or in the system.

Reinforced detection of fraud

Systematic use of red flags and their integration in processes allows for more efficient detection of irregularities and fraudulent cases. Indeed, the use of red flags in itself highlight fraud-attractive processes and point on those areas that need additional anti-fraud measures to be introduced to reduce the risk of red flags.

1



Practice 4 – Use of red flags

*This anti-fraud practice is considered a **hard detection measure** designed to mitigate both internal and external risks of fraud mainly occurring during the public procurement process, but also during the project implementation and payment. The following fraud risks are effectively detected by red flags:*

- *Rigged specification, collusive bidding, manipulation of bids;*
- *Conflict of interest;*
- *Manipulation of project costs and quality.*

This box indicates the **type of measure and the type of risks mitigated** when implementing this anti-fraud practice

Examples of the practice

ublic – Risk cards

c, the Ministries of Transports, of Industry and Trade - respectively the port, OP Maritime and Fisheries, and Innovation for Competitiveness - have adopted a common approach to integrating red flags to monitor and follow up on projects' management risks, including fraud risks. To do so, the three MAs are using so-called risk cards, which are used to ***follow-up on fraud risk indicators along the project cycle from approval to termination***. Hence, for each project co-financed under a certain OP, the MA creates a risk card.

Where MAs have delegated responsibilities to IBs, the MAs and their IBs conduct an initial common assessment of the project's red flags. The responsibility for monitoring the project's risk card is then given to IBs who regularly update it during the project cycle. MAs regularly follow up on the work of IBs on risks cards. At crucial stages of the project, MAs and IBs discuss the status of the project's risk card. This allows sharing information on new red flags identified, discussing the status of the risk management approach, and commonly agreeing on additional verifications to be carried out. Hence, during every stage of the project, IBs and MAs who perform first and second level controls on the project consult, monitor, and update the project's risk card.

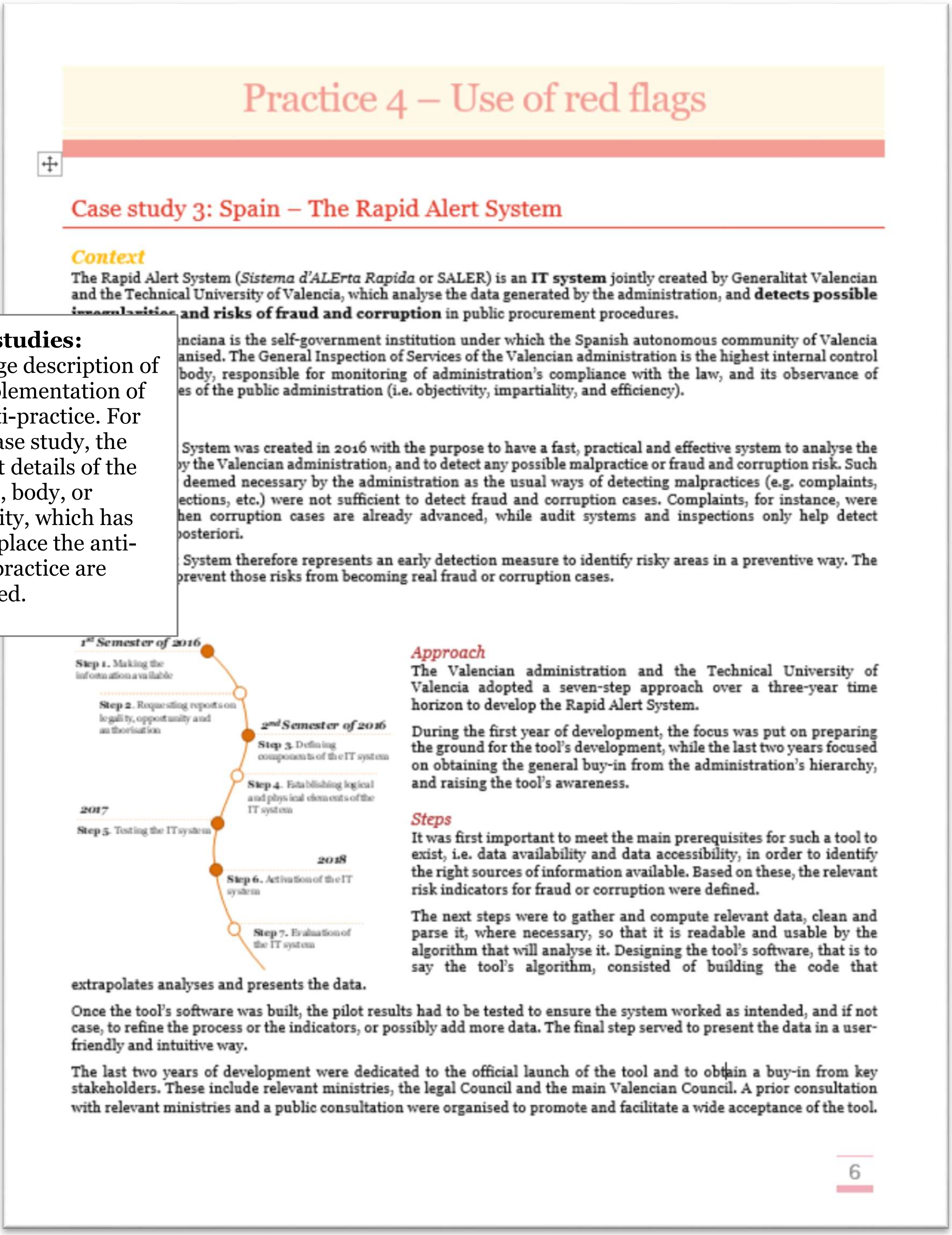
Examples:
Short descriptions of the implementation of the anti-practice in different MS.

Unique features
Similar to the methodology of the FRA recommended by the EC, the probability of the risk occurrence and the importance of the risk impact are assessed and quantified in the risks card by the person who identified the red flag. The probability of the risk occurring can range from very rare to almost certain, while the importance of the risk impact goes from imperceptible to unacceptable. Based on the assessment of each risk, the total risk of the project is quantified and reported in an ***overview table listing the total risks for each ongoing project***. In addition, a description of the risk management approach or any additional verification planned are provided, together with an indication of their status. For instance, a risk of conflict of interest within the MA during the award procedure is identified as a red flag for a specific project. The risk management approach or mitigating measure proposed would result in systematically sending results of all award evaluation to all unsuccessful applicants.

Expected impact
Since there are usually multiple project and financial managers responsible for checking the implementation of each project, risk cards serve as communication tools referencing all past red flags identified for a specific project, and indications of next steps to undertake in order to pay closer attention to certain areas seen as risky. Risk cards therefore allow the manager who conducts the verifications to know where to focus efforts.

2

Case studies:
2-4 page description of an implementation of the anti-practice. For each case study, the contact details of the person, body, or authority, which has put in place the anti-fraud practice are provided.



Practice 4 – Use of red flags

Case study 3: Spain – The Rapid Alert System

Context

The Rapid Alert System (*Sistema d'ALErta Rapida* or SALER) is an **IT system** jointly created by Generalitat Valencian and the Technical University of Valencia, which analyse the data generated by the administration, and **detects possible irregularities and risks of fraud and corruption** in public procurement procedures.

nciana is the self-government institution under which the Spanish autonomous community of Valencia anised. The General Inspection of Services of the Valencian administration is the highest internal control body, responsible for monitoring of administration's compliance with the law, and its observance of es of the public administration (i.e. objectivity, impartiality, and efficiency).

System was created in 2016 with the purpose to have a fast, practical and effective system to analyse the y the Valencian administration, and to detect any possible malpractice or fraud and corruption risk. Such deemed necessary by the administration as the usual ways of detecting malpractices (e.g. complaints, ections, etc.) were not sufficient to detect fraud and corruption cases. Complaints, for instance, were hen corruption cases are already advanced, while audit systems and inspections only help detect posteriori.

System therefore represents an early detection measure to identify risky areas in a preventive way. The prevent those risks from becoming real fraud or corruption cases.

1st Semester of 2016

Step 1. Making the information available

Step 2. Requesting reports on legality, opportunity and authorisation

2nd Semester of 2016

Step 3. Defining components of the IT system

Step 4. Establishing logical and physical elements of the IT system

2017

Step 5. Testing the IT system

2018

Step 6. Activation of the IT system

Step 7. Evaluation of the IT system

Approach

The Valencian administration and the Technical University of Valencia adopted a seven-step approach over a three-year time horizon to develop the Rapid Alert System.

During the first year of development, the focus was put on preparing the ground for the tool's development, while the last two years focused on obtaining the general buy-in from the administration's hierarchy, and raising the tool's awareness.

Steps

It was first important to meet the main prerequisites for such a tool to exist, i.e. data availability and data accessibility, in order to identify the right sources of information available. Based on these, the relevant risk indicators for fraud or corruption were defined.

The next steps were to gather and compute relevant data, clean and parse it, where necessary, so that it is readable and usable by the algorithm that will analyse it. Designing the tool's software, that is to say the tool's algorithm, consisted of building the code that extrapolates analyses and presents the data.

Once the tool's software was built, the pilot results had to be tested to ensure the system worked as intended, and if not case, to refine the process or the indicators, or possibly add more data. The final step served to present the data in a user-friendly and intuitive way.

The last two years of development were dedicated to the official launch of the tool and to obtain a buy-in from key stakeholders. These include relevant ministries, the legal Council and the main Valencian Council. A prior consultation with relevant ministries and a public consultation were organised to promote and facilitate a wide acceptance of the tool.

6. Anti-fraud practice fiches

Practice 1 – MA's monitoring system shared with other entities

Summary of the practice

One designation criteria for MAs in the 2014-2020 programming period is ensuring that all exchanges of information between beneficiaries and the MA, IBs, CA and AA can be carried out by means of electronic data exchange (As per Article 122(3) of CPR).

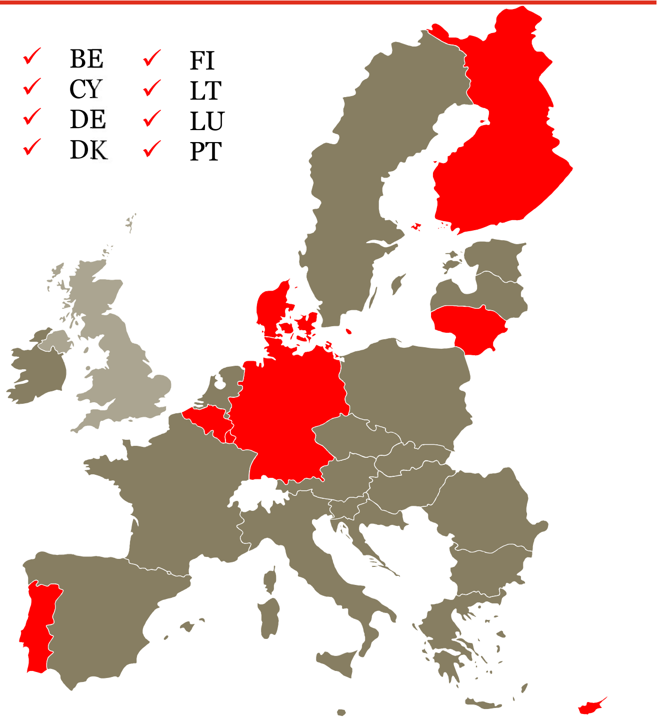
MAs have thus introduced electronic management and monitoring systems to carry out all projects' operations and sometimes, public procurement procedures.

These systems vary and can consist of completely new systems or existing information systems to which new modules and functionalities have been added to meet designation criteria. Such systems allow for the sharing of information between ESI Funds authorities and beneficiaries, as well as ensure an audit trail and a strong traceability of operations.

This anti-fraud practice presents examples of MAs which have met the designation criteria, ensuring an equal sharing of information, a fast coordination of activities, and a strong audit trail, facilitating the review by audit authorities.

Practice spotted in…

- ✓ BE
- ✓ CY
- ✓ DE
- ✓ DK
- ✓ FI
- ✓ LT
- ✓ LU
- ✓ PT



Expected impact on anti-fraud systems

Transparency

Information related to the applicant selection process is encoded and available on the platform to all relevant stakeholders depending on their access rights, thereby ensuring transparency and integrity. This information can include documents such as project appraisal analyses and reports resulting from evaluation committees and/or the project implementation phase, such as declarations of payment and other supporting documents.

Increase traceability and avoid document forgery

The archiving of documents at each stage of the co-financed project's lifecycle ensures an auditable paper trail. In some cases, documents published in the system are locked and cannot be changed after official submission to prevent possible document forgery and ensure that all users have access to the same version of the document.

Coordination between stakeholders

Such information systems ensure that the most recent information is shared between all relevant stakeholders concerned and that anyone can consult the status of an activity. In some cases, after a modification to a document or an operation is done, an automatic notification is sent through the platform to inform all relevant stakeholders.

Practice 1 – MA's monitoring system shared with other entities

*This anti-fraud practice is considered a **hard prevention** measure designed to mitigate:*

- *The risks of manipulation of projects' costs and quality; and*
- *The lack of an anti-fraud culture within an authority and, on a larger scale, within a Member State, when consistently applied by several authorities.*

Examples of the practice

Belgium – EUROGES database as a unique platform connecting all relevant stakeholders

How it works

The Walloon government is the MA responsible for OP ERDF 'Wallonia-2020.EU'. It uses the so-called EUROGES database as a platform for the coordination, management, monitoring, control and evaluation of projects co-financed by ERDF. Among other goals, EUROGES has a number of modules designed to facilitate the recording and sharing of information between stakeholders. It also keeps a record of all user activities and documents submitted, creating a clear audit trail for all operations.

EUROGES is composed of an award and a management module. The **award module** serves to carry out the evaluation and award of projects and allows sharing useful information between beneficiaries and the MA, IBs, and members of a special Task Force, which provides advice during project appraisal.

Unique features

The **management module**, allows users to manage the data collected in the selection of applicants, and collects new data specific to the monitoring of projects such as annual updates of indicators, biannual updates of projects' physical progress, and quarterly updates of projects' financial data. This information can be accessed by the services of the EC, beneficiaries, the AA, external auditors, the CA, the various actors within the MA, and the IBs, so they can monitor the progress of projects co-financed by ERDF.

The EUROGES platform also allows beneficiaries to submit standard documents to the IBs or the MA, such as receipts, project fiches, project listings, eligibility analyses etc. Users can access predefined electronic formats to create their declaration of payments, and upload scans of supporting documents such as invoices, proofs or payments, timesheets, etc.). Moreover, the system keeps a log of users' actions, and alerts the relevant authorities when a submission is made.

There is also an interface between EUROGES and the system used by the CA, allowing for the transfer of payment requests made by beneficiaries and other supporting documents.

A **public procurement module** has been created for the new programming period, enabling beneficiaries to enter a series of new, predefined data relating to their procurements as well as attach supporting documents. Once the encoding of the predefined data and supporting documents has been completed, beneficiaries can submit these to the IB or MA, which proceeds to the first level controls of the project. Opinions issued are directly encoded in the management section of EUROGES and before issuing a final opinion of its control, the MA or IB can request additional information to the beneficiary.

Finally, the platform can also be used to exchange messages between users via a **chat function**.

Expected impact

Practice 1 – MA's monitoring system shared with other entities

In March 2016, the EC verified and confirmed that all the relevant requirements regarding Article 122(3) of CPR had been met at ERDF level in Wallonia. EUROGES increases the transparency of the project data, as well as improves the traceability of the operations and reinforces coordination between key stakeholders involved in order to prevent fraudulent activities and irregularities.

Denmark – Subsidy Administration Control System (TAS) linked to the MA administration system for ERDF and ESF

How it works

The Danish Business Authority is the MA for ERDF and ESF OPs in Denmark for the 2014-2020 programming period. A joint Monitoring Committee has been established between the MA and the six Regional Growth Forums (IBs) to monitor both funds, and the MA holds the presidency of the Committee. Most of the funds are implemented in line with the recommendations made by the Regional Growth Forums established in all five Danish regions and the island of Bornholm. The Regional Growth Forums develop and prioritise actions meant to translate the regional business development strategy into specific improvements of the regional growth conditions.

The existing system for processing the ERDF and ESF enables applicants to search for all the relevant information about the funds on the managing authority's website (www.regionalt.dk). The website is continuously updated and contains general information about the funds, information about the application process, reporting requirements, requirements for settlement, etc. A project database (CVR) is also integrated in this system and contains, among other things, descriptions of all supported projects, a regional statistics bank, research articles and descriptions of the annual events.

Unique features

Information and data from project applicants are automatically fed into the MA's Subsidy Administration Control System (TAS). The regional growth forum secretariats have access to the TAS and carry out their initial case processing recommendations through this system. The MA continues its case processing in the same system. The central auditor who endorses financial statements work in the system, and the CA has access to the system to check payments requests and supporting documents. TAS contains project master data, financial data (accounts and budgets), record-keeping, categorisation/impact data and built-in management of the case flow.

When funding is awarded to an applicant, a project case is opened in the Project Reporting Application (PRV. In PRV, the project is given access to the commitment details and the project's budget, including information about a new budget every time the MA approves a change. The information is automatically transferred from TAS. From here, budgetary changes can be requested and automatically submitted to the MA for approval. In addition, information about the project's participating partners and network participants using this application is also provided.

Beneficiaries can thus submit their interim financial statements, progress reports, milestones and results, provide information about modified contact details, register participants'/employees' time use, provide information about impact, and contact the MA if they have questions via a messaging system. Recently, it has been made possible to use modules such as an accounting form/presentation of financial statements, participant/employee files, links to start-up and termination forms and result follow-up forms through PRV. In addition, it is possible to submit financial statements for projects through PRV. Efforts have also been made to develop and test a flexible reporting system based on a standard software, which will make it possible to collate all data from the various databases used in the administration of the ERDF and ESF.

Expected impact

TAS improves the traceability and audit trail of the project operations, and allows easy and transparent data sharing, and timely identification of inconsistencies in the data. Creation of one management tool can provide benefits of data centralisation and more efficient data management.

Practice 2 – Use of data collected through the MA's monitoring system to detect fraud risks

Summary of the practice

A number of MAs who use their electronic management and monitoring system to carry out and record all operations related to ESI Funds co-financed projects (see practice 1), have gone a step further in using this system. Indeed, some MAs are using data collected to detect fraudulent activities.

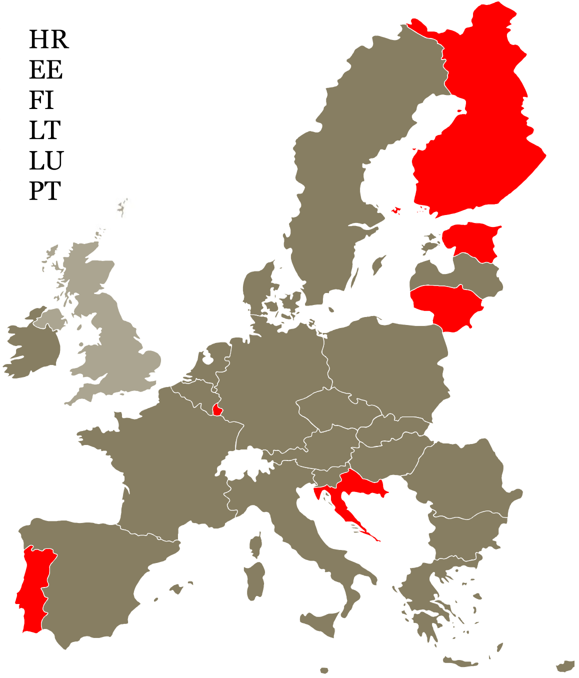
Data collected can come from:

- Operations encoded in the system by its different users including (IBs, MA, CA, Funds' applicants and beneficiaries) such as on-the-spot visit report, requests for payments and supporting documents;
- Information collected through other databases and registers publicly available (e.g. tax register, criminal register, etc.), or interoperable with the system (e.g. e-procurement platform, certified bidders register) needed to verify applicants' eligibility in the applicant selection stage.

The most common fraud risks that MAs and IBs can detect via this system by using the data collected through it, include double funding applications and manipulations of project and labour costs.

Practice spotted in...

✓ HR
✓ EE
✓ FI
✓ LT
✓ LU
✓ PT



Expected impact on anti-fraud system

Strengthened checks in the selection of applicants

When verifying the eligibility of fund applicants, MAs and IBs need to have access to a variety of data on the applicant. Interoperability between the MA monitoring system and other national databases provides a rapid and efficient way to collect this information in a short timeframe as well as reinforce the checks performed on fund applicants.

Reinforced management verifications during project implementation

During project implementation, a significant amount of data is required and exchanged between beneficiaries, IBs, MAs, and CAs. For instance, payment requests submitted by beneficiaries and accompanied by supporting documents such as timesheets, enables verification of possible manipulations of project and labour costs.

Increase administrative compliance and fraud detection

The once-only principle, enabled by interoperability, contributes to reducing errors and irregularities and consequently strengthening administrative compliance. Hence, when a malpractice is detected, MAs and IBs are more attentive to red flags and fraud risks.

Practice 2 – Use of data collected through the MA's monitoring system to detect fraud risks

*This anti-fraud practice is considered a **hard detection measure** designed to mitigate both external risks of fraud, mainly occurring during the selection of applicants, but also during the project implementation and payments. The anti-fraud practice can effectively detect the following fraud risks :*

- *Double funding;*
- *Manipulation of project costs and quality.*

Examples of the practice

Finland – EURA 2014 to detect double funding and manipulation of project and labour costs

How it works

EURA 2014 is the electronic management and monitoring system for projects co-financed by the ESF and ERDF for the programming period 2014-2020 in Finland. The Finnish Ministry of Employment and the Economy manages EURA 2014. MA, IBs, CA, AA, applicants and beneficiaries, which have access to this system (see Practice 1).

The system primarily serves to ensure traceability of all projects' operations i.e. selection of applicants, project implementation and verifications, and payments and certifications. The system records and archives all data input by its users during these phases, such as follow-up and final reports, preparation and receipt of project management decisions, etc. The system also stores all documentation from management verifications (e.g. on-the-spot visit's reports) and documentation for EC reporting.

The EURA 2014 system follows the so-called once-only principle, which means that once information has been provided by a user once, there should be no need to input it again. The once-only principle also enables users to pre-fill documents on the basis of the information previously provided by s project's applicant and beneficiary. All documents produced by EURA 2014 are solely archived in electronic form.

Unique features

The system includes direct access to the tax authority website (vero.fi) and links to other relevant authorities. The company registration numbers for all new applicants are sent on a daily basis from the EURA 2014 database to the tax authority's database in order to get extensive information on the tax debts of the applicant. The tax debt information is checked from the EURA 2014 database before funding decisions are made.

In addition, EURA uses data from projects' operations to perform the following countermeasures related to the detection of fraud:

- The same invoice cannot be entered twice in the MIS, which avoids double funding applications;
- Concerning labour costs, the MA can use the system to check whether the same staff member was working less than the required number of hours per day, across all projects;
- The system automatically prevents the same person being declared as staff for more than one project;
- The timesheet completed by staff working on projects must include all projects in which the person is involved.

Expected impact

EURA 2014 management and monitoring system offers various functionalities including greater efficiency in procedures and reduction of administrative burden and traceability of project's operations. In addition, thanks to data stored in EURA 2014, MAs and IBs can perform fraud detection activities, including checking for double funding applications and detecting possible manipulations of project and labour costs.

Practice 2 – Use of data collected through the MA's monitoring system to detect fraud risks

Portugal – Balcão 2020 to detect double funding

How it works

The "Balcão 2020" is system is the point of access and monitoring system for all OPs co-financed by ESI Funds for all entities wishing to apply for project financing. The system also performs the selection of applicants and project implementation. Balcão 2020 was developed by the Agency for Development and Cohesion to be used as a communication platform between ESI Funds authorities and applicants that participate in the OPs Portugal 2020. This system is used to manage all applications and entities under the ESIF programmes and its development started in previous programmes (2007/2013). This tool has several integrated modules used in the application process.

Unique features

The main module that manages eligibility factors for applications is the business register ("Base única de Promotores"). This module aims to **identify double funding applications by project applicants**, which is against the principle of sound financial management, one of the key requirements for ESIF applicants. In case a double funding application is detected, the applicant is forbidden to submit a new application for a defined period of time.

This module also uses information associated with the applicant, located in several public administration databases, namely:

- The Tax Authority;
- The Social Security;
- The Judicial Authority;
- The National Register of Certified Beneficiaries, IAPMEI).

The result of this process establishes the classification of the entities in two dimensions. One related to the suitability and reliability code of the applicant (inhibited, conditioned, indicted or suitable), and the other related to the debt (in terms of ESIF recovery procedures) code of the applicant (entity not eligible or eligible entity). This information is only available in detail for the MA, ADC, CA and AA.

However, the set of tools and modules used within Balcão 2020 do not perform any checks for adverse media searches about applicants or other referred entities.

Expected impact

The interoperability of Balcão 2020 with other national systems and databases enables IBs and MAs to perform checks for double funding applications, and ensure that the applicant is eligible for funding and complies with the principle of sound financial management.

Practice 3 - Cooperation between ESI Funds authorities and other national authorities

Summary of the practice

Cooperation between ESI Funds authorities and other key national anti-fraud stakeholders brings several benefits to the fight against fraud and corruption. In its guidelines for preparing national anti-fraud strategies for ESI Funds, the European Commission emphasises the value of strengthening prevention measures for competent authorities in MS.

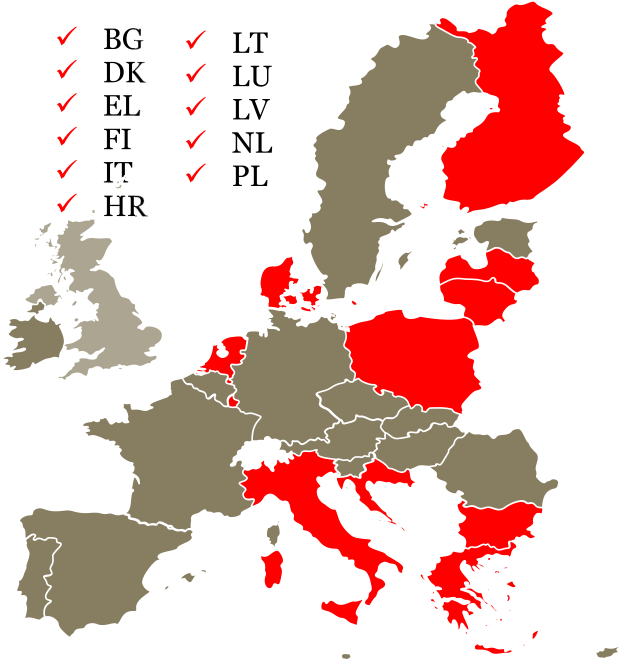
To make prevention more effective, closer and faster, cooperation between all relevant stakeholders and an overall enhanced coordination of action are highly encouraged.

Cooperation can be achieved through various mechanisms, such as the creation of working groups, informal networks of authorities, and formal and informal cooperation agreements.

Examples presented in this practice cover some of the cooperation mechanisms put in place under the initiative of MS competent authorities.

Practice spotted in…

- ✓ BG
- ✓ DK
- ✓ EL
- ✓ FI
- ✓ IT
- ✓ HR
- ✓ LT
- ✓ LU
- ✓ LV
- ✓ NL
- ✓ PL



Expected impact on anti-fraud system

Synergies

An important benefit from such cooperation mechanisms is the synergy arising from the regular exchanges of information and discussions on risks and potential controls to be implemented. The collaboration also enables the devising of tools and procedures that better target identified areas of risks. It also reduces the duplication of work and allows an alignment of strategies for fighting fraud and corruption.

Knowledge sharing

Establishing close links through common workshops, presentations or trainings with other relevant bodies enables the sharing of knowledge and the development of a common understanding with counterparts. Such events are important in ensuring all bodies are informed about new risk areas, are trained or made aware of potential fraud schemes and ways to identify these. Knowledge sharing also fosters peer learning and leads to an increased capacity of all parties involved.

Coordination between stakeholders

Greater cooperation among bodies often leads to greater coordination, which is crucial in fighting fraud and corruption. Indeed, practices identified show that coordination with authorities such as law-enforcement authorities can lead to a better identification and reporting of fraud cases by combining efforts and building on various stakeholders' expertise. In essence, improved coordination leads to more efficient and more effective common operations.

Practice 3 - Cooperation between ESI Funds authorities and other national authorities

*This practice is considered as a **soft prevention** anti-fraud measure, primarily helping to mitigate a lack of skills and reinforce an anti-fraud culture within an authority and at the national level, as well as support the capacity building of anti-fraud practitioners within competent authorities. In addition, cooperation mechanisms are considered to have an indirect, positive impact on the detection of all fraud risks. This is due to the sharing of knowledge and information, which contributes to awareness raising on fraud indicators amongst participating authorities, allowing them to take timely take relevant actions.*

Examples of the practice

Croatia – Network for the Management of Irregularities

How it works

Croatia has a decentralised management system of ESI Funds involving several IBs. The Ministry of Regional Development and EU Funds of Croatia is the MA responsible for the OP Competitiveness and Cohesion. It has delegated responsibilities to nine first and second level IBs, to which duties and obligations significantly vary as they relate to different priority axes, and thereby requires the monitoring and control of very different projects.

In order to prevent the occurrence of irregularities and fraud cases and to exchange good and bad practices in the handling, reporting and follow-up on irregularities, the Ministry of Finance has established a Network for the Management of Irregularities.

Unique features

The initial Network meeting took place in February 2017, and in general, the meetings are to be held regularly every three to four months or earlier if needed. The Network includes staff for irregularities in second level IBs, irregularity coordinators in first level IBs, and where appropriate, other representatives of IBs, representatives from the Agency for the Audit of European Union Programmes Implementation System and experts from the Ministry of Economy, Entrepreneurship and Crafts, as well as the Directorate for Public Procurement Policy.

Network for the Management of Irregularities is a forum that gathers practitioners and sets up an arena for discussion. The Network allows stakeholders to share practices and experiences, discuss cases of irregularities, reflect on common trends and changes, and focus of irregularities.

Involvement of the stakeholders from different levels (central authorities and IBs) creates the opportunity for them to raise the questions, request additional guidance and have a better visibility on the overall process of irregularities management and roles and responsibilities of each stakeholder. The organisation of the regular meetings of the Network is the key to its success, as timely and coordinated knowledge sharing allows for more efficient detection of irregularities and their effective management.

Expected impact

Croatia's implementation of the Network for the Management of Irregularities is expected to benefit all stakeholders involved. Potential benefits may include the enhancement of competences related to fraud detection, better coordination between stakeholders of different levels, shorter feedback loops, faster and more efficient decision making, and improved peer learning between the IBs.

Practice 3 - Cooperation between ESI Funds authorities and other national authorities

Lithuania – Cooperation with the Financial Crime Investigation Service

How it works

To ensure a sufficient flow of information between the MA, the AA and the CA, a cooperation agreement between these authorities and the Financial Crime Investigation Service (FCIS) has been established. Trainings and workshops are organised, particularly between those three authorities but also with the Special Investigation Service (SIS).

Unique features

The Board of the Illegal Support Prevention and Investigation is the main unit of FCIS, involved in the coordination with the ESI Funds authorities. The Board of the Illegal Support Prevention and Investigation seeks to strengthen the competences of the management and control system institutions. In addition, it actively shares information about the trends in criminal acts and newly emerging fraudulent mechanisms, and offers preventive measures.

The Board of the Illegal Support Prevention and Investigation organizes meetings of the Working Group of Irregularity Officers for the ESI Funds authorities. These meetings provide the possibility to exchange on best practices, deal with current issues and solve emerging problems.

The meetings with the Irregularity officers are attended by representatives of IBs, ministries and the SIS, among others. These meetings take place on a quarterly basis as a means to exchange information on fraud prevention measures, planning processes and developing anti-fraud tools. The number of institutions having Irregularity Officers has constantly increased since the 2004-2006 programming period from 15 to 22 for the 2014-2020 programming period.

Expected impact

The practical cooperation with the investigation services and law enforcement institutions in Lithuania is expected to reinforce the practical skills of fraud detection and thereby improve the Irregularity Officers' understanding of the fraud implementation mechanisms as well as detection and investigation. Moreover, such cooperation influences the assessment of fraud risks and fosters better targeting of measures in light of evolving fraud practices.

Practice 3 - Cooperation between ESI Funds authorities and other national authorities

Italy – Memorandum of understanding between the Ministry of Economic Development and the Financial Police

How it works

On 21 January 2014, the Ministry of Economic development and the Financial police of Italy signed a memorandum of understanding in order to formalise their cooperation. It focused, among other areas of collaboration, on the "investments projects and programs of administrations, entities and individuals that avail of both public and European funds as well as the national subsidies, also cofounded by the European Union, in relation to incentives being benefited from firms in disparate sectors".

Expected impact

In this light, the collaboration between the Ministry of Economic Development and the Special Unit of Financial Police on public expenditure and repression of European frauds strengthened the prevention aimed at curbing fraudulent activities and smoothened the exchange of information. In addition, the Ministry of Economic Development, when needed, may also call on the above-mentioned Special Unit for the conduction of investigations, checks and monitoring.

Lithuania – Knowledge transfer with the Financial Police of FYR Macedonia

How it works

Building the capacity in fraud detection can benefit not only from national exchange, but also from international collaboration. An example of such successful collaboration is a twinning project between Lithuanian authorities, led by the Financial Crime Investigation Service, and the Financial Police within the Ministry of Finance of FYR Macedonia.

The project was executed in November 2015- May 2016 as part of the European Union IPA 2011 Programme, with a budget or EUR 250,000. It gathered five authorities from Lithuania (the Ministry of Finance, the Central Project Management Agency, Financial Crime Investigation Service, Special Investigation Service and the Prosecutor General's Office) involved in the detection and investigation of financial crimes.

The objective of the project was to improve the national capacities of the Finance Police for protection of the EU financial interests and cooperation with the European Anti-Fraud Office (OLAF). In addition, this project aimed at improving the national legal framework, reinforce administrative capacities of the national institutions and strengthen cooperation within the system for fight against fraud and irregularities of ESI Funds.

Unique features

In the scope of the twin project, the representatives from the public administrations of Lithuania and FYR Macedonia worked together in order to transfer the expertise and good practices developed within the EU.

Experts from Lithuanian institutions shared their experience and, in cooperation with the colleagues from Macedonia, developed recommendations on how to improve the practices of the Financial Police on Macedonia when dealing with fraud and corruption in ESI Funds, supported drafting relevant procedures, conducted trainings targeted trainings for the staff of the Financial Police and organised study visits in Lithuania.

Expected impact

The bilateral project between public authorities from Lithuania and FYR Macedonia contributed to the development of an effective and efficient system of protection of EU financial interests in FYR Macedonia and reinforced its cooperation with the European Anti-Fraud Office (OLAF).

This project represents a successful practice of sharing knowledge and experience between several countries and thereby increasing the capacity of local authorities in the field of fraud detection for ESI Funds operations.

Case study: Danish AFCOS network

Context

Under the new Regulation No 883/2013 (OLAF Regulation), which came into force in October 2013, all Member States were required to designate an Anti-Fraud Coordination Service (AFCOS). In May 2014, the Danish Ministry of Finance was appointed AFCOS, and at the same time, an AFCOS network was established at the national level ensuring adequate and close coordination between Danish authorities relevant to the fight against fraud and corruption.

Objective

The Danish AFCOS network ensures fast and sound cooperation in the fight against fraud and corruption in Denmark, and provides a valuable input to the functioning of the Danish AFCOS.

Structure

In addition to transferring fraud cases of an administrative nature from the Danish competent authorities to OLAF, the Danish AFCOS also chairs the network, which is composed of the following authorities:

- Danish Agricultural Agency under the Ministry of Environment and Food.
- Danish Fisheries Agency under the Ministry of Foreign Affairs
- Danish Business Authority , regional unit under the Ministry of Business and Growth
- Danish Tax Authority (SKAT)
- Danish State Prosecutor for Serious Economic and International Crime (SOIK) under the Ministry of Justice.

These authorities consist of the Danish authorities in charge of managing the EU spending programmes, collecting the Danish contribution to EU own resources (customs), as well as investigating and prosecuting criminal cases of fraud in EU funds.

How it works

Members of the Danish AFCOS network usually **meet three times a year** - in January, May and October - or as needed, and the goal of these meetings serves various purposes related to the fight against fraud.

First, these meetings help **ensure a regular top-down and bottom-up communication** between the Commission and national ESI Funds authorities on anti-fraud issues. For instance, the network meets to prepare and agree on the content and information to report to the Commission, which constitutes an input to the PIF report.

Case study: Danish AFCOS network

Such meetings also serve to **disseminate knowledge and information stemming from the Commission** to all members of the network. Following a meeting of the Advisory Committee for the Coordination of Fraud Prevention (COCOLAF) for instance, members of the network meet to discuss information and updates from the EC level, and agree on the best approach to disseminate this information to staff members of all relevant authorities e.g. discussing follow up measures to PIF report recommendations.

Similarly, these meetings also present an opportunity to **share fraud related knowledge obtained or produced by members of the network**. For instance, sharing a presentation from the Ministry of Justice on data protection law and its impact on the work of competent authorities in combating fraud and corruption, or disseminating the annual report from the European Court of Auditors on their major audit findings.

Finally, members of the AFCOS network meet to **share and benefit from the feedback, experience and practices** implemented, which have led to a successful anti-fraud outcome such as the detection of a fraudulent case. Successful approaches and processes used by managing authorities which have led to the identification of certain patterns of fraud, or the detection of real fraud cases, are regularly shared within the network and widely disseminated to benefit other managing authorities or other authorities.

In addition to regular and ad hoc meetings, members of the AFCOS network have concluded several **informal cooperation agreements**, and in some cases with external parties. These cooperation agreements primarily serve to:

- **Reinforce the detection of double funding**. A cooperation agreement has been concluded between the Danish Business Authority and the Danish Agriculture Agency under the Ministry for Food, Agriculture and Fisheries on the issue of **double funding**. Twice a year, the Danish Business Authority supplies data to the Ministry on companies, which have received funding. The Ministry for Food, Agriculture and Fisheries further checks for double applications. Should a suspicion remain after the check is completed, the case manager from the Danish Business Authority is informed and can request additional verifications.

- **Support specific sectors of economy.** A similar cooperation agreement has been concluded in June 2014 between the Danish Agriculture Agency and the Danish Tax Authority (*SKAT*) on **agricultural support and EU market organisations**. The goal of this agreement is to create a framework for ongoing cooperation and dialogue in relation to agricultural support and EU Common Market Organisations.

- **Provide harmonised and comprehensive anti-fraud responses**. A third cooperation agreement has been concluded between SKAT, the national police, and the Attorney General. The goal of this agreement is to create a framework for constructive cooperation between the three parties, where authorities jointly ensure an effective, correct and uniform task solution and continuously strive to facilitate cooperation. Notably, close cooperation between relevant managers and employees of the three authorities is fostered to ensure effective and comprehensive action against economic, organised and cross-border crime, border control, customs, investigation and enforcement of criminal matters. The cooperation takes the form of coordinated efforts, discussion and planning of priorities, common focus on specific actions, and information exchange and assistance.

Expected results

The Danish AFCOS network brings about several benefits:

- Increased and faster cooperation and reaction of member Authorities, leading to an increased awareness and exchange of knowledge and good practices related to fraud and corruption risks, patterns, cases identified, etc.;

Practice 3 - Cooperation between ESI Funds authorities and other national authorities

Case study: Danish AFCOS network

- Fast and informal communication between member Authorities who are more comfortable and prone to engage with colleagues from a different Authority and informal discussions;
- Due to its informal nature, the network is very agile and can thus be adjusted dependt on the need, and can involve additional non-member Authorities if need be.

The creation of the AFCOS network did not entail the signing of any formal or written cooperation agreements from the participating Authorities. Rather, the network was created upon a government decision, following the 2013 OLAF Regulation and the requirement to designate an AFCOS.

Contact details

Name of the entity: 5th Division - International Cooperation and Defence, Ministry of Finance of Denmark

Website: www.fm.dk

Email address: fm@fm.dk

Practice 4 – Use of red flags

Summary of the practice

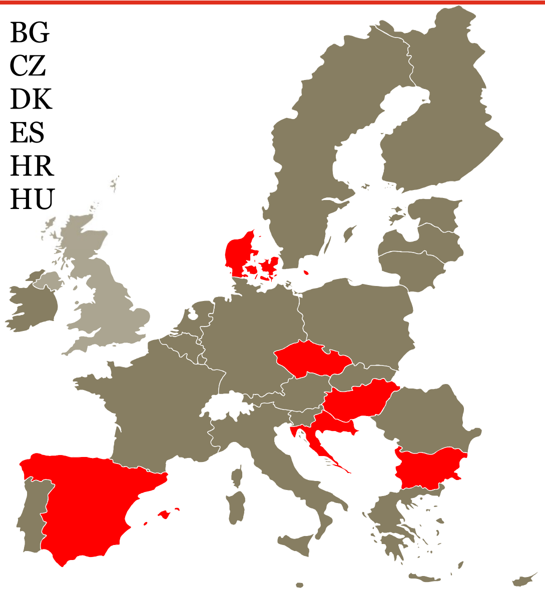
Red flags are defined by the Commission and OLAF as a set of circumstances that are unusual or vary from normal activity and may indicate **warning signs, hints, and indicators of possible fraud or irregularities**. OLAF is in charge of elaborating an overview of fraud risks and associated red flags.

In several MS, MAs have either integrated OLAF's red flag list into their verification checklists, or they have expanded it to create their own list. While relying on OLAF guidance increases the capacity of MAs and IBs to recognise red flags, the examples described in this anti-fraud practice go a step further. They focus on authorities that have implemented a more systematic and efficient use of red flags.

Measures developed by MAs and IBs in using red flags range from integrating a **predefined list of red flags into their management verification checklists**, to creating more advanced IT tools such as, **data analytics tools** capable of detecting red flags early enough to foresee relevant mitigating actions.

Practice spotted in…

- ✓ BG
- ✓ CZ
- ✓ DK
- ✓ ES
- ✓ HR
- ✓ HU



Expected impact on *anti-fraud system*

More harmonised and targeted management verification procedures

When red flags are integrated into checklists or systems, verifications performed by IBs and MAs are improved and procedures are more **standardised and evenly applied**. In addition, the staff of the IBs and MA can apply targeted red flags to specific projects or beneficiaries. Therefore, MAs and IBs staff are more cautious and thorough in conducting checks, and verifications become more project or beneficiary-specific, thereby increasing the likelihood of detecting any possible deviations from normal activity and practice. In some MAs, specific additional checks are foreseen when some red flags are detected.

More consistent approach in performing management verifications

When red flags are documented in a checklist or a system, and do not only rely on staff's experience, changes of personnel have less impact on the quality of the controls. Similarly, several staff members working on the same project or with the same beneficiary can obtain the same level of knowledge about fraud risks related to a project or a beneficiary by simply looking at the checklist or in the system.

Reinforced detection of fraud

Systematic use of red flags and their integration in processes allows for more efficient detection of irregularities and fraudulent cases. Indeed, the use of red flags in itself highlight fraud-attractive processes and point on those areas that need additional anti-fraud measures to be introduced to reduce the risk of red flags.

Practice 4 – Use of red flags

*This anti-fraud practice is considered a **hard detection measure** designed to mitigate both internal and external risks of fraud mainly occurring during the public procurement process, but also during the project implementation and payment. The following fraud risks are effectively detected by red flags:*

- *Rigged specification, collusive bidding, manipulation of bids;*
- *Conflict of interest;*
- *Manipulation of project costs and quality.*

Examples of the practice

Czech Republic – Risk cards

How it works

In Czech Republic, the Ministries of Transports, of Agriculture, and of Industry and Trade - respectively the MAs for OP Transport, OP Maritime and Fisheries, and OP Enterprise and Innovation for Competitiveness - have adopted a common approach to integrating red flags to monitor and follow up on projects' management risks, including fraud risks. To do so, the three MAs are using so-called risk cards, which are used to ***follow-up on fraud risk indicators along the project cycle from approval to termination***. Hence, for each project co-financed under a certain OP, the MA creates a risk card.

Where MAs have delegated responsibilities to IBs, the MAs and their IBs conduct an initial common assessment of the project's red flags. The responsibility for monitoring the project's risk card is then given to IBs who regularly update it during the project cycle. MAs regularly follow up on the work of IBs on risks cards. At crucial stages of the project, MAs and IBs discuss the status of the project's risk card. This allows sharing information on new red flags identified, discussing the status of the risk management approach, and commonly agreeing on additional verifications to be carried out. Hence, during every stage of the project, IBs and MAs who perform first and second level controls on the project consult, monitor, and update the project's risk card.

Unique features

Similar to the methodology of the FRA recommended by the EC, the probability of the risk occurrence and the importance of the risk impact are assessed and quantified in the risks card by the person who identified the red flag. The probability of the risk occurring can range from very rare to almost certain, while the importance of the risk impact goes from imperceptible to unacceptable. Based on the assessment of each risk, the total risk of the project is quantified and reported in an ***overview table listing the total risks for each ongoing project***. In addition, a description of the risk management approach or any additional verification planned are provided, together with an indication of their status. For instance, a risk of conflict of interest within the MA during the award procedure is identified as a red flag for a specific project. The risk management approach or mitigating measure proposed would result in systematically sending results of all award evaluation to all unsuccessful applicants.

Expected impact

Since there are usually multiple project and financial managers responsible for checking the implementation of each project, risk cards serve as communication tools referencing all past red flags identified for a specific project, and indications of next steps to undertake in order to pay closer attention to certain areas seen as risky. Risk cards therefore allow the manager who conducts the verifications to know where to focus efforts.

Practice 4 – Use of red flags

Croatia – EC-recommended red flags integrated into management verifications

How it works

Croatian regulation sets the requirement for all MAs of ESI Funds and their IBs to use red flags for carrying out their management verification procedures. More specifically, the EC's Information Note of Fraud Indicators for ERDF, ESF, and CF (COCOF 09/0003/00-EN) has been transposed into the Common National Rules (CNR) for Management and control system of MAs in Croatia. Implementation of the CNR is expected to reinforce the use of red flags and identification of fraud risks for OPs under ESI Funds.

Application of CNR in the part of red flags is done through implementation of EC-recommended fraud risks indicators, tailored fraud risks indicators or by using IT tools. The case of latter, the MA responsible for the OP Competitiveness and Cohesion reinforces the project risk assessment and red flag identification using Arachne risk scoring tool. For this OP, The MA has introduced procedures for the use of Arachne in the CNR No.6 and No.10. However, all the functionalities offered by Arachne are not yet fully used by Croatian authorities. Those mostly used by the MA include identification of relations between legal entities and/or persons in order to identify possible conflict of interest.

Unique features

The MA for the OP Competitiveness and Cohesion integrated a ***list of 16 fraud schemes and their associated red flags*** into management verification checklists during desk-based and on-the-spot checks. The type, degree and frequency of the verifications using those red flags depend on the assessed level of risk for the project. Hence, the higher the perception of fraud risks for a specific project, the stricter the verifications will be. For instance, a project assessed with a high degree of riskiness could be subject to more frequent on-the-spot checks, involving more targeted verifications.

To follow up on the implementation and monitoring of fraud risks, the MA has designated ***risk coordinators*** in charge of coordinating with project managers of IBs on the use of red flags in their management verifications

Therefore, IBs are required to use the red flags in monitoring the following websites:

- The e-procurement website on the Public Procurement Office website;
- The State Commission for Control of Public Procurements' website.

In addition, IBs carry out ***ex-ante and ex-post verifications*** of public procurement documentation, in which they also pay close attention to red flags. Methodology for conducting ex-ante and ex-post verifications also foresees the use of Arachne, based on the risk analysis related to individual procurements, ensuring that all procurement with estimated value equal to or higher than EU thresholds are selected for ex-ante verifications.

Moreover, IBs also integrate red flags when verifying and approving applications for reimbursement submitted by beneficiaries. During this process, IBs verify all submitted applications for reimbursement and choose a sample of claimed costs for additional verifications.

Expected impact

Requirement of integration of red flags into the management and control system in Croatia ensured a high standard for risk control and verification for ESI Funds operation. The list of red flags covering 16 fraud schemes ensure that all the risky areas of the project cycle are regularly monitored and investigated. Moreover, implementation of IT tools for identification of red flags for key risk areas suggest more efficient and effective identification of irregularities and potential fraudulent cases.

Practice 4 – Use of red flags

Denmark – Red flags to assess and categorise companies

How it works

The Danish Business Authority, the MA responsible for ERDF and ESF OPs during the 2014-2020 programming period, and its six regional IBs, integrate red flags into their management verification checklists. In addition, authorities have tailored specific red flags for assessing and classifying companies during the selection of applicants and the implementation phase of the project. The assessment of companies is performed using the MA's monitoring system and external databases. Identification of the risky areas is based not only on the knowledge and experience of MA staff but is also reinforced through the knowledge exchange with other MAs through Danish AFCOS network of national bodies (see Case study in anti-fraud practice 5).

Unique features

Red flags are used during the company assessment to collect information on indication of business, geographical, legislative, and economic nature, and cover the organisation structure, history and business relationships of companies at stake. Once sufficient information on a company has been collected, the MA and IBs categorise companies into one of the four groups:

1. Companies unwilling to comply with the rules;
2. Companies unwilling to comply with the rules but may be affected;
3. Companies willing to comply with the rules but do not have the ability to do so; and
4. Companies willing to comply with the rules and have the ability to do so.

These categories were developed on the basis of the following indicators:

- Track records on irregularities;
- Filing of complaints;
- Knowledge and skills to comply with the rules;
- Organisational structure;
- Level of confidence in the authority.

This structure is dynamic and flexible, allowing company to be moved into a different group if a change of behaviour occurs. This system allows the Danish Business Authority and its six IBs, to use a similar approach in assessing fund applicants and bidders.

Expected impact

Danish Business Authority believes that the red flag system fosters a strong ethical culture and a zero tolerance approach to fraud. The system allows authorities regularly exchange information on suspicion of fraud, identified potential fraud patterns and good practices in fighting fraud and corruption. In addition, the flexible nature of the system creates the need for periodic fora and workshops where authorities discuss the developments and behavioural changes of selected companies, thus reinforcing the cooperation and capacity building among authorities.

Hungary – The Red Flags early warning system

How it works

The Red Flags www.redflags.eu tool is the result of an initiative started in 2013 between Transparency International Hungary, the K-Monitor Watchdog Organisation for Public Funds and the PetaByte IT Research Company. The tool was launched in 2015 with the purpose of bringing more transparency to the Hungarian public procurement system by creating an IT system capable of generating automatic alerts whenever a contract notice or contract award notice seems suspicious or may contain corruption or fraud risks. It is funded by the European Commission under the HERCULE programme, as part of a larger effort to address procurement risks in several MS.

Unique features

Tender notices and contract award notices are the main source of structured information on procurement. Therefore, the Red Flag tool relies on tender notices and contract award notices published in Tenders Electronic Daily (TED) to automatically monitor and control procurement expenditure in Hungary. This is made possible thanks to an algorithm that allows to filter areas where procurements are at risk. The algorithm has been developed around a set of 40 indicators that are considered as risk factors by Transparency International Hungary, from which 32 are used to check contract notices and 9 are used to check award notices.

When looking at contract notices, indicators such as technical capacity and economic and financial ability requirements as well as the use of specific procedures considered favourable ground for corruption are assessed to determine whether the notice contains risk factor(s). For contract award notices, indicators can include procedures without prior publication, the ratio of the total final value and estimated value, or unsuccessful procedures for risky reasons or without statement of reason.

For the risk analysis, the tool makes a distinction between 'red flags' and 'pink flags'. The 'red flag' indicators are directly linked to contract or award notice data related to a specific procurement procedure. These red flags may indicate an actual infringement or a simple risk. On the other hand, 'pink flags' are not linked the specific procurement procedure but refer to previous instances, which increase the risk profile of either the contracting authority or the economic operator. They are based on information collected in previous research or from external sources of information (e.g. government databases) and serve to complement the red flags. For instance, they can inform on whether the contracting authority has been convicted by a final judgement or provide information on the conduct of the winning bidder.

Every signal sent by the Red Flags tool cannot be considered as an evidence for corruption. These signals should be considered as a gauging mechanism that advise on areas of a tender or award notice where special attention should be paid. In cases where several signals are received for the same notice of award notice, then this may suggest a greater likelihood that corruption exist.

Expected impacts

The Red Flags tool is considered very promising, as it is the first of its kind. Despite its limited coverage of procurement expenditure, i.e. above thresholds, it represents an effective tool for detection of fraud risks for the stake of project procurement and increase of its transparency. The tool currently has over 700 registered users in Hungary and its application is being considered by civil society organisations in several other MS.

Italy – National Anti-fraud Database (future implementation)

In order to introduce an IT system for risk analysis, complementary to those of the Commission (Arachne, IMS, etc.), the Italian Central Anti-Fraud Coordination Office (AFCOS) has planned the development of a special electronic application, known as DNA (National Anti-Fraud Database), whose purpose is to strengthen the fight against fraud in Italy.

In order to design and develop an efficient tool, a **preliminary benchmarking** of all existing databases used for the monitoring and control of EU funding in Italy was carried out, both at central and local level by the competent authorities. In addition, the **feasibility of the creation and use of the DNA by all ESI Funds authorities** has been assessed, with the specific purpose of detecting irregularities and fraud.

The national anti-fraud IT application will consist of a single platform compiling data from different sources. In particular, the data included in the application should come from two types of sources: (i) information on the use and destination of EU financing streams held by the Authorities (or Bodies) responsible for managing them and (ii) information that is cross-checked and combined with the data in the information databases, in order to carry out risk analysis.

The full scale implementation of the tool is expected in 2020

Practice 4 – Use of red flags

Case study: Spain – The Rapid Alert System

Context

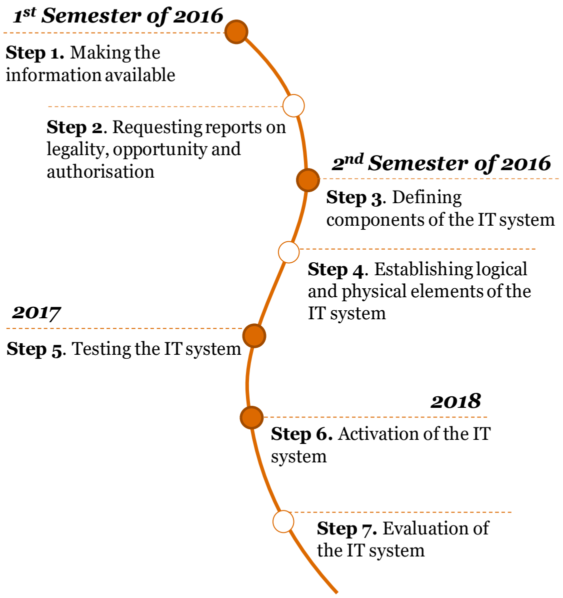
The Rapid Alert System (*Sistema d'ALErta Rapida* or SALER) is an **IT system** jointly created by Generalitat Valencian and the Technical University of Valencia, which analyse the data generated by the administration, and **detects possible irregularities and risks of fraud and corruption** in public procurement procedures.

Generalitat Valenciana is the self-government institution under which the Spanish autonomous community of Valencia is politically organised. The General Inspection of Services of the Valencian administration is the highest internal control and inspection body, responsible for monitoring of administration's compliance with the law, and its observance of general principles of the public administration (i.e. objectivity, impartiality, and efficiency).

Objective

The Rapid Alert System was created in 2016 with the purpose to have a fast, practical and effective system to analyse the data generated by the Valencian administration, and to detect any possible malpractice or fraud and corruption risk. Such tool was largely deemed necessary by the administration as the usual ways of detecting malpractices (e.g. complaints, audits and inspections, etc.) were not sufficient to detect fraud and corruption cases. Complaints, for instance, were usually filed when corruption cases are already advanced, while audit systems and inspections only help detect irregularities a posteriori.

The Rapid Alert System therefore represents an early detection measure to identify risky areas in a preventive way. The system aims to prevent those risks from becoming real fraud or corruption cases.


1st Semester of 2016
Step 1. Making the information available
Step 2. Requesting reports on legality, opportunity and authorisation
2nd Semester of 2016
Step 3. Defining components of the IT system
Step 4. Establishing logical and physical elements of the IT system
2017
Step 5. Testing the IT system
2018
Step 6. Activation of the IT system
Step 7. Evaluation of the IT system

Structure

Approach

The Valencian administration and the Technical University of Valencia adopted a seven-step approach over a three-year time horizon to develop the Rapid Alert System.

During the first year of development, the focus was put on preparing the ground for the tool's development, while the last two years focused on obtaining the general buy-in from the administration's hierarchy, and raising the tool's awareness.

Steps

It was first important to meet the main prerequisites for such a tool to exist, i.e. data availability and data accessibility, in order to identify the right sources of information available. Based on these, the relevant risk indicators for fraud or corruption were defined.

The next steps were to gather and compute relevant data, clean and parse it, where necessary, so that it is readable and usable by the algorithm that will analyse it. Designing the tool's software, that is the tool's algorithm, consisted of building the code that extrapolates, analyses and presents the data.

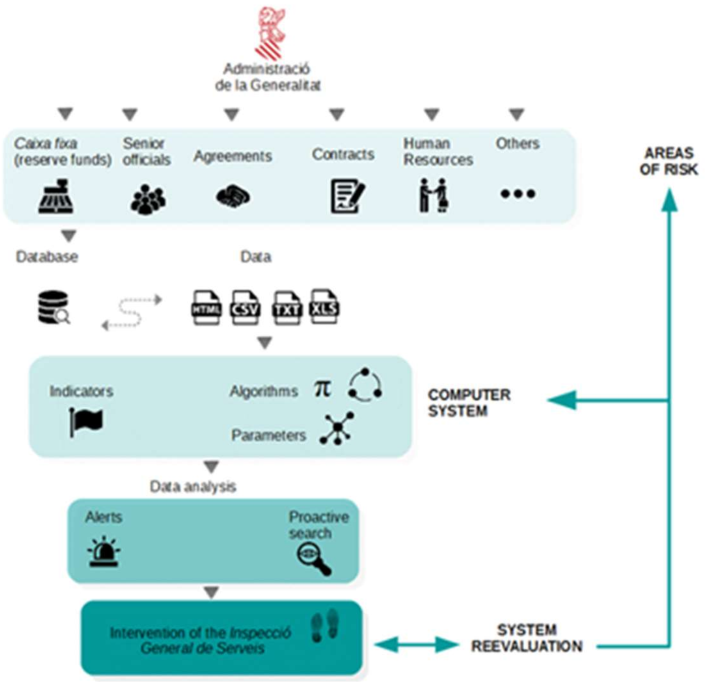
Practice 4 – Use of red flags

Case study: Spain – The Rapid Alert System

Once the tool's software was built, the pilot results had to be tested to ensure the system worked as intended, and if not case, to refine the process or the indicators, or possibly add more data. The final step served to present the data in a user-friendly and intuitive way.

The last two years of development were dedicated to the official launch of the tool and to obtain a buy-in from key stakeholders. These include relevant ministries, the legal Council and the main Valencian Council. A prior consultation with relevant ministries and a public consultation were organised to promote and facilitate a wide acceptance of the tool.

Once the buy-in was obtained, the final step was to create a legal basis for the Rapid Alert System, and for the General Inspection of Services of the Valencian administration that will be responsible for the use and management of the tool. The legal basis will also indicate sanctions related to cases detected by the Rapid Alert System. The draft law was submitted and is currently in parliamentary procedure. It is expected to be approved this year upon which, the use of the Rapid Alert System will be activated.



How it works

The Rapid Alert System **interconnects information from files containing administrative data**, allowing the system to identify areas of risk.

Risk indicators

Indicators are established on the selected data and parametrised using algorithms. This further allows revealing correlations by cross-referencing the data. Indicators include both quantitative and qualitative elements. **Quantitative indicators** are converted into numerical parameters that make it possible to set automatic alerts (e.g. unjustified period payments to the same company, or double application for subsidies). **Qualitative indicators** identify the modus operandi of possible bad practices based on the study of past cases (e.g. organisational deficiencies related to responsibilities and functions).

When an alert is triggered, the action protocol of the General Intervention Services is activated. In addition to signalling alerts, the system **enables proactive searches** and the **evaluation of results**.

Information sources

Information feeding the Rapid Alert System come from both internal and external databases to which the administration has access. Internal information sources include files such as records of contracts (data relating to all phases of the bidding process, implementation of the contract and complaints where relevant), direct payments (data related to the types of products or services acquired and suppliers), subsidies (data relating to the holder of the body granting the subsidy, conflicts of interest, beneficiary, justification, and invoices). External databases consists of the register of declarations of activities and goods held by high officials, notarial information from the Valencian tax administration, the register of the controlling bureau for conflict of interest, and databases with personnel and payroll data. Monitoring these records and databases does not imply any legal obstacle as the information stored is public.

Defining accurate and **specific risk indicators serving as red flags is key to identify** irregularities and fraud cases. Some of them are easy to identify such as, VAT numbers, contract references, payment date, and references in records regarding gifts, trips etc., while some others are more complex and require knowledge of apparently unrelated processes taking place at the same time. Each department of the Valencian administration has developed its own set of indicators and identified risk factors associated with their procedures. All data provided by individuals or companies applying for public calls for tender, and interacting with the public administration will be digitalised to further reinforce these indicators.

An alert is triggered when an objective risk is detected. All alerts are registered, and when **an investigation is launched**, it results in monitoring activities or a case being filed. Investigations consist of identifying weaknesses in the system, coding ongoing situations, and improving existing and adding new indicators. This continuous process is key to the success of the Rapid Alert System.

Expected results

The Rapid Alert System brings about several benefits. First, it acts as **a firebreak to counteract inertia and malpractices** within the Valencian administration by enabling a consistent and systematic way of monitoring of past and present irregularities and fraud cases. Based on real detected cases, the tool allows **identifying some patterns**, which give indications of where follow-up is most needed. Second, the Rapid Alert System and more specifically the legal basis around it which provides for sanctions, fosters an ethical culture amongst public employees, bidder and beneficiaries of the Valencian administration.

During its pilot, the tool has already demonstrated its capacity and efficiency in detecting fraudulent cases. The type of irregularities and fraud risks the Rapid Alert System has been able to identify include among others, split purchases and more specifically unjustified separation of purchases, conflict of interest, and collusive bidding.

Some lessons learnt

The development and implementation of the Rapid Alert System has been facilitated by several key success factors including:

- Data availability - which is a binding prerequisite to develop such system;
- Access to the right information sources - without them key indicators cannot be computed;
- Early buy-in of stakeholders - as it is key to obtain all necessary data;
- Creating a legal basis needed to provide legal coverage to the inspection staff when they request data.

.

Contact details

Name of the entity: Generalitat Valenciana

Website: www.gva.es/

Email address: generalitat_en_red@gva.es

Name of the entity: Technical University of Valencia

Website: www.upv.es/

Email address: informacion@upv.es

Practice 5 – Whistleblowing mechanisms

Summary of the practice

Whistleblowing policies are a means to encourage individuals to reporting unethical, criminal or unlawful activity to authorities by offering them protection from reprisals.

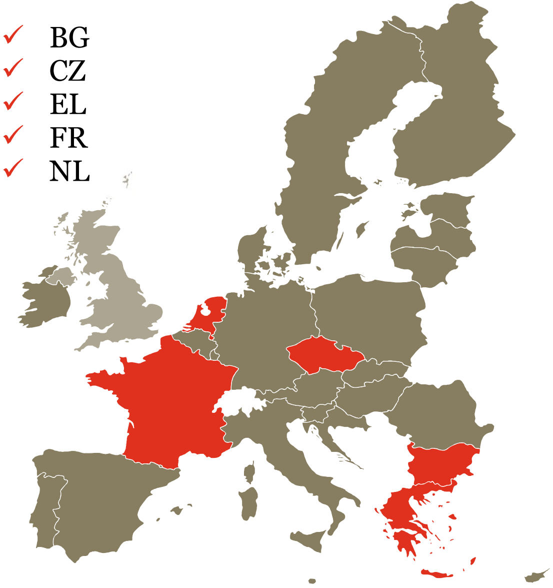
A clear and well-enforced policy of whistleblower protection policy is an essential part of a comprehensive anti-fraud approach. Whistleblowing mechanisms differ between MS and OPs and can take a form of an **email channel, a dedicated web-page** at the MA or centralised level, or, in some, cases, a **regional or a national web-platform** that coordinates whistleblowing channels of several authorities.

A comprehensive whistleblowing policy should be built on a strong national whistleblowing legislation, and provide authorities with clear internal structures and procedures on how to stimulate and protect whistle-blowers, as well as how to follow up and investigate the whistleblowing alert.

The policy examples below represent effective implementation of several forms of whistleblowing policy at the national and fund level. However, some forms of whistleblowing policies were spotted in all MS.

Practice spotted in…

- ✓ BG
- ✓ CZ
- ✓ EL
- ✓ FR
- ✓ NL



Expected impact on *anti-fraud system*

Enhanced fraud detection

Effective whistleblowing mechanisms allow authorities to identify cases of potential fraud or irregularities as well as evidence for their further investigation. In combination with internal anti-fraud measures implemented by the MA or IB, the whistleblowing reinforces the detection of fraud and provides important data on the misconduct that at the early stage, allowing for effective control.

Reinforcement of anti-fraud culture and ethical behaviour

An effective and well-developed whistle blowing system creates the pre-conditions for the more responsible and transparent management of the funds. It reinforces the anti-fraud culture at the level of the beneficiaries and at the level of responsible authorities. Moreover, it is an important driver of ethical behaviour in the workplace.

Strengthening internal controls

The potential for a whistleblowers' accusation to lead significant financial and reputational damage. As such, the mere presence of a whistleblower policy, and of a culture that rewards and protects whistleblowers can also act as an incentive for beneficiaries to reinforce internal anti-fraud controls.

Practice 5 – Whistleblowing mechanisms

*This anti-fraud practice is considered a **hard detection measure** designed to reinforce the detection of fraud and to strengthen the anti-fraud environment and ethical culture. Implementation of the whistleblowing mechanisms has transversal impact and covers all risk categories across all the stages of the project cycle.*

Examples of the practice

France – ELIOS platform

How it works

In the context of the Art 125(4)(c) of the CPR and Art. 59 of the EU Financial Regulation (Regulation (EU) No 966/2012) the managing authority for the Operational Programmes for Employment and Inclusion in Metropolitan France (FSE) and Youth Employment Initiative (YEI), has developed the so-called ELIOS whistle-blowing platform.

The ELIOS platform is a website composed of a homepage and two main sections allowing to make a whistleblowing alerts:

- Whistleblowing alert on fraud,
- Whistleblowing alert on conflict of interest.

Unique features

The homepage of the platform provides users with information on the legal basis of whistleblowing protection. It also contains links for the whistleblowing form and for two possible topics for whistleblowing: fraud and conflict of interest. For each of the topics, explanation and definition of fraud, conflict of interest and related misconduct is provided.

The platform's homepage contains a link to access the whistleblowing form. However, before the user can access the actual form, the platform requires a 3-step confirmation procedure, includes warnings on:

- During the first step, the ELIOS platform states that the user can report a suspicion regarding projects of ESF or YEI only. The platform is not is not competent for reporting other European funds (EAFRD / EMFF) nor for programs managed by regional management authorities (Regional Council ERDF / ESF programs). The whistleblowing platform provides users with guidance on where to address the inquiries related to topics not related to ESI Funds (e.g. tax evasion, contribution fraud and social benefits, customs fraud or fraud in the labour code)
- The second step contains a warning on the consequences and legal responsibility for false reporting;
- The third step includes detailed description of the legal basis for whistle-blower protection.

The user has to confirm the understanding of all warnings before accessing the whistleblowing form.

Finally, the platform requires the whistleblower to provide his personal information. Therefore, anonymous whistleblowing is not possible on the ELIOS platform. Users can file a claim up to six months after the date of the incident.

Expected impact

The development and implementation of the ELIOS platform allows to :

- Centralize all complaints, regardless of the management department concerned;
- Trace the filing of the complaints (registration and acknowledgment of receipt);
- Transfer claims to relevant manager services for processing;
- Allows to follow-up with the whistle-blower on the case.

Thus, the ELIOS platform supports the detection and the reporting of the risks of fraud on the site of the MA to allow whistle-blowers to have a single entry to signal anonymous and secure signalling of fraud and conflict of interest.

As a result, the availability of a centralized whistleblowing platforms for ESF and YEI funds creates additional tool for fraud detection, improves the trust to the MA and created a feedback loop with the beneficiaries and the general public.

Bulgaria - Whistle Blowing of Irregularities under EU Projects

How it works

The Ministry of Finance (MoF) is the body responsible for implementing the whistleblowing policy in relation to the EU projects in Bulgaria. The EU projects whistleblowing mechanism webpage (http://www.minfin.bg/en/375) is a go-to information source for whistleblowers. It contains the contact information on the relevant bodies for the whistleblowing for different Funds and programmes, as well as procedures and requirements for successful whistleblowing.

The MoF's webpage on irregularities contains guidance for a person that wants to blow the whistle in relation to EU funded projects. The webpage is structured around several key topics:

- Definitions of irregularities, suspected fraud and fraud;
- Key responsible authorities and their functions;
- How to blow the whistle;
- Procedures to follow up the submitted whistle blowing alert;
- Specific features regarding alerting the irregularities.

Unique features

The MoF lists the distribution of the tasks and scope of activities of the National Funds Directorate and Centralised Contracting and Public Procurement Directorate in relation to the management of funds and dealing with the irregularities and fraud.

The webpage suggest several ways to blow the whistle:

- Directly contact the relevant MA;
- Fill in the form and submit it though the website of the MoF;
- Send a free-form email at the email address provided.

In addition, any oral or written alerts may also be submitted.

The MoF guarantees the anonymous submission of the whistleblowing alert though all the channels, including oral and written channels. Similarly, the web-form does not require submission of personal data by the whistleblower.

The webpage provides clear indications on the minimum amount of information to be included in the whistleblowing alert. It should include at least clear reference to the specific project, the financing programme, the administrative unit and a description of the irregularity.

Next, the guidance to the whistle-blowers provide the legal basis for the whistle-blower protection and the procedure how the alert will be followed up. It gives the whistle-blower an opportunity to be informed personally on the status of his/her request, if contact details were provided during the submission of the request.

Upon submission of the alert on irregularities to the National Fund Directorate, the system generates a reference number and an access code. The whistle blower can use this information to follow up on the alert. Moreover, one can check the status of the whistleblowing alert directly on the website of the OF by entering the specific reference number and an access code of the alert.

Expected impact

The centralization of the information of the possible whistleblowing channels at the website of the MoF allows systematising the approach for different authorities and funds. Moreover, it suggests to the user single point of contact and single information source of different aspects of the whistle blowing policy. Such approach will increase the chances of the user to find a reliable channel for whistleblowing.

In addition, the whistleblowing is encouraged by providing numerous ways to blow the whistle and anonymous nature of posting an alert. MoF improves the transparency of the follow up on the alert by providing the user the access to the status of the case investigation by entering the alert details on the website.

Practice 6 – Practical anti-fraud training

Summary of the practice

Enhancing the skills and anti-fraud capacity of authorities dealing with ESI Funds is seen as a general need throughout Europe.

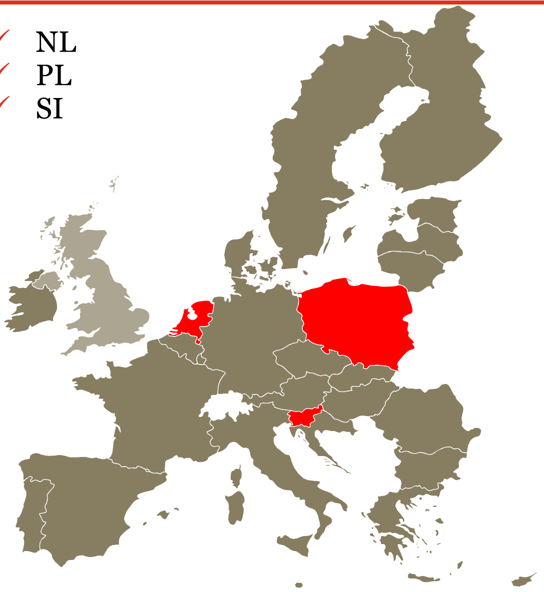
Training courses are the most common form of capacity-building exercise as they can be implemented in several ways and produce rapid tangible results when they are designed in a practical manner and based on real-life case studies. A wide range of involved parties including public bodies, NGOs and highly experienced anti-fraud auditors have designed such anti-fraud training courses.

Existing anti-fraud training courses have been designed in different formats that are more or less interactive, i.e. on-site training, e-learning modules, immersion seminars fostering peer-to-peer exchange, and investigation games. The scope of these training courses varies from basic introductory sessions to more targeted anti-fraud courses.

Examples of anti-fraud training courses under this practice include those designed with anti-fraud investigation services of the police and experienced anti-fraud investigators from audit authorities.

Practice spotted in…

- ✓ NL
- ✓ PL
- ✓ SI



Expected impact on anti-fraud system

Enhanced anti-fraud capacities and skills

Practical training courses based on real-life fraud cases help participants to enhance specific fraud-detection capacities and skills. In addition to teaching techniques and procedures to identify red flags and fraud schemes, training also helps participants to develop an affinity for detecting cases of fraud and corruption, which usually only experience can bring.

Earlier detection of fraud and corruption cases

Increased anti-fraud capacities and skills results in the ESI Funds authorities being more proactive and cautious. This means that they can detect fraud indicators in a more timely fashion, thus allowing them to take relevant measures to avoid potential fraud and corruption from becoming a reality.

Sharing of anti-fraud good practices

Training that encourage the interactivity and the participation of attendees usually allow time for informal peer-to-peer exchanges. These interactions mean that experience and good practices can be shared and the experience of other authorities can be enhanced.

This anti-fraud practice is considered a ***horizontal soft prevention measure*** *that has an impact on all types of fraud risk, primarily by increasing the anti-fraud capacity of authorities' staff members.*

Practice 6 – Practical anti-fraud training

Examples of the practice

Poland – Training delivered by the Central Anti-Corruption Bureau

How it works

Poland's Central Anti-Corruption Bureau (CBA) is a special government body with police and monitoring powers. The CBA's objective is to combat corruption in the public and private sectors, particularly in governmental institutions and local governments and, more generally, in every activity that endangers the State's economic interest. The CBA has 850 fraud investigators and 150 civil servants.

Based on the pressing need for anti-fraud training identified while investigating fraud cases, and on the extensive experience gained, the CBA has decided to invest in the creation of anti-fraud training.

Initially, the CBA created an on-site anti-fraud introductory training course based on its previous anti-corruption guide for public officials. The training course aimed to raise awareness among public officials, clerks, public administrations and businesses of corruption. To do so, the content of the training course was based on real-life case studies. As part of the training, participants learn about possible behaviours to adopt when dealing with corruption. Participants are also provided with more topic-specific training material prepared by the CBA, such as recommendations on anti-corruption proceedings by using public procurement procedures.

Unique features

In addition to on-site training, the CBA has created an anti-corruption e-learning platform. First launched in May 2014, this platform is the first free e-learning platform in Poland, accessible only using a username and password. The platform was developed with the financial support of the European Commission (EC) as part of the Prevention of and Fight against Crime Programme. The goal of this e-learning platform is to raise participants' awareness of corruption within public administrations and businesses, as well as raising society's awareness of anti-corruption efforts in Poland. The platform consists of three theme-based blocks covering corruption in public administration, corruption in business, and the social impact of corruption. Those with access to the platform may take any of the three training courses corresponding to these blocks. Online training consists of no more than 10 chapters, each of which contains an informative part and a test. The test must be passed in order to move on to the next chapter. The trainings is available in Polish and English.

Expected impact

Only three months after the e-learning platform was launched, 4,500 persons were already registered on the platform; and after 12 months, this figure rose to 22,000. Between May 2014 and November 2017, 46,626 people took the training course on corruption in public administration. In November 2017, the CBA decided to modernise the platform, and 10 months after the new platform was launched, there were 61,272 members. The platform currently has 126,757 members who have enrolled on one of the training courses, 25,017 of whom have completed the course on corruption in public administration since the new platform was launched. These statistics demonstrate the interest and need for more anti-corruption training in Poland and elsewhere.

The CBA has plans for the future: a train-the-trainer programme will be developed to scale up on-site training courses, the content of the e-learning platform will be modernised, and a new technical solution will be implemented. An international universal e-learning platform with national plug-ins is also under development.

Practice 6 – Practical anti-fraud training

Slovenia – Training for fraud investigators and criminalists to improve fraud detection and investigation

How it works

In 2013, the Ministry of the Interior of the Republic of Slovenia coordinated and benefited from the THEMIS project funded by the EC as part of the Prevention of and Fight against Crime (ISEC) programme. The objective of this two-year project was to improve the overall knowledge and increase the skills and capacities of fraud investigators and criminalists working for the Slovenian police, as well as judges dealing with financial crime and suspicions of fraud and corruption in the detection and investigation of EU co-financed projects.

To do so, targeted parties were provided with valuable and necessary insight into the complex system of EU funding, thus allowing them to perform their work more efficiently and effectively. More specifically, participants were provided with relevant and comprehensive information on:

- The EU funding in the 2007-2013 programming period;
- Respective national implementing structures of the programming period, the MCS, key parties involved and their roles and functions;
- Different programmes and funding from different agencies;
- The new set-up of national implementing structures for the 2014-2020 programming period.

In addition, training participants received a structured compendium with a systematic overview on funding and implementing structures for each target group.

Unique features

The method used to train the target groups consisted of a series of interactive and participative workshops covering the following themes:

- Fraud detection by MAs, IBs, AAs and Corruption Prevention Commissions, in the context of Structural and Cohesion funds management;
- Crime intelligence and detection and investigation of fraud cases; and
- International cooperation of police authorities to protect the EU's financial interests.

Those attending the workshops signed up for an immersive experience as the workshops were held over a short period. Therefore, participants were invited to stay on site so that they could attend all the workshops. Those that did so were able to enjoy informal conversations, ask questions and share their experiences and good practices with others participants. These interactions were seen as a positive and valuable outcome of the THEMIS project.

In addition, participants were invited to take part in panel discussions and presentations on management verifications and relevant funds. Sharing of real-life examples as well as active participation during Q&A sessions was encouraged.

Expected impact

The Ministry of the Interior participated as a Slovenian MA in the series of workshops covering fraud detection in the context of Structural and Cohesion funds management. Following these training sessions, the MA was able to identify tangible benefits of the THEMIS project.

A general increase in and closer cooperation between ESI Funds authorities and the police was noted. This led to additional capacity-building initiatives and training provided to authorities by the police on the fraud prevention and detection. This then resulted in an earlier detection of fraud by ESI Funds authorities' staff members, and more structured risk management and control procedures.

Practice 6 – Practical anti-fraud training

Case study: The Netherlands –Anti-fraud game

Context

The anti-fraud game is a highly interactive and engaging anti-fraud training course developed to build the capacity of all ESI Funds' authorities to prevent, detect and combat fraud and corruption. The anti-fraud game was created by Jo Kremers, a Senior Audit Manager working in the Dutch Ministry of Finance, using his extensive experience gained from working as a fraud investigator for the private and public sectors, and then as an auditor.

Rationale

During the previous and current programming period, Jo Kremers detected several cases of fraud and misuse of ESI Funds, which were never detected by the Dutch MAs. The lack of general knowledge on the anti-fraud cycle and the need for increased knowledge and capacity in setting up a robust anti-fraud system were the first elements indicating the strong need for anti-fraud training in preventing, detecting and combatting fraud.

This led to a realisation in the importance of raising ESI Funds authorities' awareness of the reputational damages fraud and corruption cases can cause, and the need to enhance their anti-fraud capacity by providing them with the right instruments, methods and tools to combat fraud.

Objective

While developing the anti-fraud game, the aim was to create a highly interactive game relying on several multimedia tools such as videos, music, pictures and animations, and attributes in order to:

- Draw and retain the attention of participants during the entire session;
- Foster a rapid and lasting learning process by associating a concept or information taught with a sound, image, video or object.

Therefore, the aim is neither to provide a classical training course covering EU laws and regulations, nor to provide them with a set of ready-to-use anti-fraud measures that they can directly integrate into their management and control system procedures. Instead, the anti-fraud game training was invented with the aim of motivating and encouraging participants and developing their ability to identify red flags of fraud and corruption by being more aware, attentive and responsive to hints and cues of fraud, thereby allowing them to put in place the most appropriate and effective anti-fraud control measures.

Target group

The anti-fraud game focuses on the wide group of ESI Funds stakeholders, including MAs, IBs, the CA, the AA from all EU Member States, EU candidate countries, and more generally practitioners working with EU and national funds. However, it can easily be adapted to a single stakeholder group or a mix thereof. A game session includes a maximum of 35 to 40 participants.

Format

The anti-fraud game is divided into two parts:

1. Part I – Game for sub-groups;
2. Part II – Individual game.

Practice 6 – Practical anti-fraud training

Case study: The Netherlands –Anti-fraud game

The training course generally starts with a plenary session, during which the trainer breaks the ice among participants by raising participants' awareness of their lack of knowledge of the anti-fraud cycle. After the plenary session, participants are put into mixed sub-groups and the first part of the game can start. Placing participants into sub-groups early on in the session encourages the start of discussions and the sharing of experience. Moreover, mixing different authorities into a sub-group helps them understand each other's obligations and challenges.

To encourage the start of discussions, the trainer uses real-life cases of fraud and corruption in ESI Funds that have been anonymised and used as test cases. The second part of the game is a plenary session involving all participants. Participants work individually on 12 test cases based on real (realistic) cases of fraud and corruption in ESI Funds. The test cases are designed to improve the group's skills and use of instruments, and raise awareness of the importance of ethics and integrity.

Unique features

An important aspect of fraud detection, yet one that is more difficult to understand, is successfully **developing an affinity for detecting cases of fraud and corruption**. In addition to using checklists and making on-the-spot verifications, participants need to learn how to better observe and understand the environment in which they operate and where fraud could possibly occur. Hence, participants need to learn how to rely on and trust their common sense, and build on their experience by being exposed to different settings and a range of fraud schemes.

The anti-fraud game is a multimedia training course that uses pictures, videos, music and animation associated to the variety of topics covered in the course. Indeed, linking a visual or sound to a topic makes it more attractive to participants who grasp the shared knowledge and information more quickly and thus remember it more easily. The use of tokens and attributes is also encouraged as it also improves their learning process and memory retention.

In order to spark participants' interest and motivation, awards and prizes are offered to participants at the end of the training course.

Delivery mode

The anti-fraud game is played in various educational institutions throughout Europe, e.g. the European Academy for Taxes, Economics & Law in Berlin or the International Anti-Corruption Academy in Vienna. The training course has also been given during some EU-level events such as the Annual Symposium EU Funds in Berlin, and following ad-hoc requests made by EU Member States and candidate countries, including Belgium, Germany, Latvia and Macedonia. Finally, Jo Kremers also gives the training to the Dutch Ministry of Finance's audit department.

Expected results

As new technology is changing, fraud techniques and corruption methods are becoming more advanced, thus making them more difficult to detect. Players of the anti-fraud game will therefore learn how to move away from the traditional formal ways of detecting cases of fraud and corruption, and will develop a unique ability that allows them to pay more attention to the least obvious signs of fraud. The anti-fraud game has shown promising results in promptly increasing the capacity of authorities to detect fraud and irregularities at different stages of the project cycle.

Contact details

Name of the trainer: Jo Kremers

E-mail address: jmwkremers@home.nl

Practice 7 – Cooperative approaches to conducting the FRA

Summary of the practice

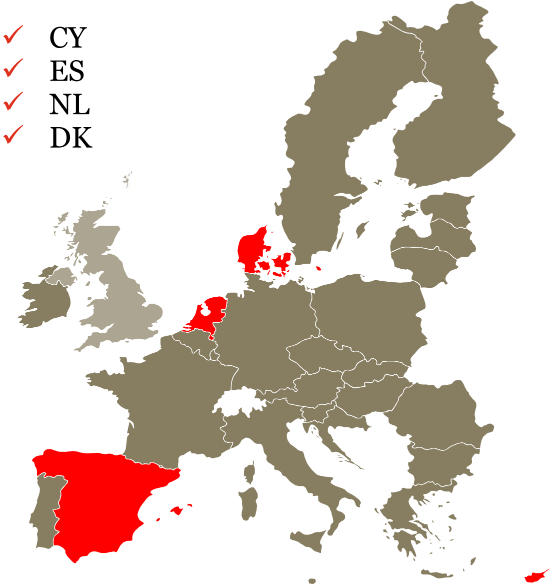
Several managing authorities (MAs) across the EU have adopted a **cooperative approach when organising their Fraud Risk Assessment (FRA) process. It consist of working together to develop an FRA and support the intermediary bodies (IBs)** with the performance thereof. This resulted in a consistent and coordinated approach to analysing fraud and corruption risks, and to setting up effective and proportionate measures to mitigate the risks identified, thereby increasing the potential of those measures in the fight against fraud and corruption.

This practice particularly concerns Member States where **MAs) have delegated functions and responsibilities to their IBs**, which therefore must also carry out an FRA. It also specifically concerns MAs and IBs that have **chosen to use the template prepared by the European Commission (EC) to conduct the FRA**.

This anti-fraud practice provides examples of such set-ups, which have facilitated the uptake and conduct of FRAs by several bodies, and adopted a team-based approach to discussing fraud risks and related mitigating measures.

Practice spotted in…

- ✓ CY
- ✓ ES
- ✓ NL
- ✓ DK



Expected impact on the anti-fraud system

Common and better understanding of fraud risks and anti-fraud measures

When processes that clearly define management and controls procedures and put in place anti-fraud measures are run in parallel, the learning process is accelerated. In addition, the parties involved tend to better and more rapidly understand the importance of the FRA process by linking it to the well-organised management and control system.

Increased transparency

A comprehensive manual of procedures, such as the Blue Book, helps increase transparency of management and control procedures (including anti-fraud procedures) among all the parties involved. In addition, since all of these parties have a clear vision of their functions and responsibilities, this increases their accountability in day-to-day tasks.

Improved compliance and mitigated reputational risks

Since the transparency of procedures and the accountability of the authorities' staff members who implement them are improved, there are fewer errors and irregularities, thereby minimising the reputational risk of authorities.

*This anti-fraud practice is considered a **horizontal soft prevention measure** that has an impact on all types of fraud risk, primarily by increasing the anti-fraud capacity of authorities' staff members.*

Practice 7 – Cooperative approaches to conducting the FRA

Examples of the practice

Cyprus – Cooperation between MAs and IBs

How it works

The Directorate-General for European Programmes, Coordination and Development of the Republic of Cyprus is the MA responsible for most of the country's OPs. It has delegated some of its functions to four categories of IBs in the country. To conduct the FRA, the MA has chosen to use the template proposed by the EC and to transpose it for use by the IBs.

Before conducting the assessment, the MA set up a **single self-assessment team for all OPs,** including staff members from the MA responsible for financial management and control, staff members from IBs responsible for project selection and on-the-spot verifications specifically, the control authority (CA), the Anti-Fraud Coordination Service (AFCOS), and the Public Procurement Directorate of the Treasury of the Republic of Cyprus. Members of the self-assessment team were selected to include those who have relevant experience in all basic functions covered by the management and control system (MCS) of the OPs. In addition, a member of the audit authority (AA) was selected to be an observer of the entire FRA process.

The self-assessment team based its FRA on the list of fraud risks identified by the EC and followed the five-step methodology proposed by the EC. However, the self-assessment team customised all fraud risks to its context, together with the mitigating control measures that it tailored according to the MCS.

Unique features

The self-assessment team was divided into subgroups to cover the risks and measures pertaining to a specific FRA process. For instance, a subgroup involving IBs responsible for project selection focussed on risk and mitigating measures related to the "Selection of Applicants" section in the FRA, while another subgroup was in charge of the "Implementation and Verification" section. The CA was responsible for addressing risks and mitigating measures related to the "Certification and Payment" section.

The MA organised a meeting gathering all members of the self-assessment team to explain the overall structure, purpose and benefits of the FRA. Several meetings and sub-group meetings were subsequently held to explain in more detail how the assessment should be completed. These on-request meetings between the MA and the self-assessment team or between the MA and the sub-groups were beneficial, as some members found the terminology used in the FRA not always straightforward or mitigating measures not always applicable to the specific context of IBs.

Expected impact

Cooperation between authorities when conducting the FRA provided a comprehensive overview of the ESI Funds' MCS for OPs, as well as a better understanding of existing procedures and mitigating measures applied by all the parties involved, at all levels and for all OPs. The MA was able to obtain a full overview of the checks implemented by the IBs in the country, while IBs had the opportunity to discuss their specific set-up in detail with the MA and other IBs. The resulting FRA confirms this cooperation, as it includes an additional "Comments" column used by all members of the self-assessment team to explain when a mitigating measure proposed by the EC was not relevant to the IB context, or simply to describe the status of the mitigating measure. This is seen as very proactive and useful for conducting future FRAs as it will be easier to make corrective changes and re-evaluate the risks.

Practice 7 – Cooperative approaches to conducting the FRA

The Netherlands – Cooperation between MAs of European Structural and Investment Funds (ERDF)

How it works

The four ERDF MAs in the Netherlands adopted a coordinated and cooperative approach when conducting their FRA. When setting up their anti-fraud system, the four ERDF MAs had already organised joint meetings with the CA, AA and the Ministry of Economic Affairs and Climate and Ministry of Finance, where relevant, to discuss and agree on an anti-fraud system and ensure that all MAs act in the same way in similar circumstances. For instance, the MAs have set up common checklists for all ERDF MAs and IBs. Discussions only take place when all the authorities involved are present. It is in the context of these regular meetings that the FRA was conducted.

Unique features

The self-assessment team was composed of the four ERDF MAs and the CA. The AA was not part of the self-assessment team, instead acting as an observer of the overall process. The meeting regarding the FRA became a one-day workshop. The workshop was initially intended to set up the common approach for completing the FRA and screen the mitigating measures recommended by the EC, in order to identify those that needed to be tailored to the context of the OPs. The self-assessment team therefore used a mix of EC-recommended mitigating measures and customised measures. This workshop also allowed the four MAs to share their experience on the most important fraud risks in their environment as well as express their views on the most relevant mitigating measures, in order to address them in their context. As the four MAs used the FRA template proposed by the EC, some parts were filled in as a team, while others were filled in individually during the one-day workshop. The four ERDF MAs jointly filled in the “Selection of Applicants” and “Implementation and Verifications” sections, while the CA filled in the “Payments and Certification” one. With regard to the direct procurement process, the four ERDF MAs completed it individually in separate documents and following the dedicated workshop. However, the MAs did not work in silos to complete this last process, as each one shared its completed process with the others in order to obtain feedback and suggestions for improvements.

Expected impact

This type of cooperation is not only valuable to the FRA by the Dutch authorities, but also to the country’s general anti-fraud system. Sharing experiences and practices between the MAs of one fund is expected to lead to a better coverage of risks, improved communication from the authorities and a more coordinated implementation of anti-fraud measures. As a result, it should enhance the overall anti-fraud system for ERDF fund management in the country.

Practice 7 – Cooperative approaches to conducting the FRA

Case study: Spain – Coordinated approach to create a compendium of anti-fraud procedures of the MA, CA and IBs

Context

The **Blue Book** is the comprehensive manual of procedures of the MA for ERDF to describe all the functions and procedures related to the management and control system of the 21 OPs under its responsibility. The Blue Book is developed by the MA together with the CA, in order to support the designation requirements (as per Article 124 of the Common Provisions Regulation (Regulation (EU) No 1303/2013).

ERDF management is highly decentralised in Spain, with the MA only managing 5% of ERDF funding. **A large part of the MA's functions is therefore delegated to IBs**. The main tasks of IBs include, among others, the selection of operations, ex ante verification of expenditure, submission of applications for payment to the MA, and communication with beneficiaries. IBs also support the MA in all its remaining functions. They are composed of **13 central government bodies** (e.g. ministries and public specialised agencies), **25 regional authorities** (e.g. the Government of Valencia) and **more than 100 'light IBs'** that consist of local administrations implementing integrated projects for urban development and are only responsible for selecting operations. As a result, IBs perform different operations involving very distinctive management and control system procedures, and are thereby prone to different fraud and corruption risks.

2014-2020

Descripción de funciones y procedimientos de la Autoridad de Gestión y la Autoridad de Certificación

VERSIÓN FINAL

"Una manera de hacer Europa"

Approach

Since the MA must ensure the quality of all IBs' control and management systems and supervise the tasks delegated to them, it **adopted a two-fold approach** to do so. First, it requested that each **IB prepare its own Blue Book** describing the procedures for the control and management system specific to its context. Second, the MA required **all IBs to align the methodology in conducting their FRA, to tailor the mitigating measures proposed by the EC to their specific aspects,** and document the methodology and anti-fraud measures put in place in the annex to their Blue Books.

Objective

The objective of this approach was to cope with the decentralised management and control of ERDF OPs in Spain and to ensure that all IBs follow the same procedures under similar circumstances. To do so, the MA **put together a compendium of all the monitoring and control procedures and anti-fraud measures implemented by the MA, CA and IBs in order to obtain an overview at ERDF level, thereby ensuring transparency and the compliance of procedures**. Increasing transparency, awareness and compliance of such procedures also encourages the MA, CA and IBs' staff members to pay closer attention to irregularities and red flags that could possibly indicate fraudulent activity.

The individual IBs' Blue Books supplement the one produced by the MA and CA. Together, they provide an overview at OP level of all the management and control system procedures for the 21 ERDF OPs. They also summarise the legal framework for MA and IBs referring to the obligation to put in place anti-fraud measures that are based on the common tools and proposed set of mitigating measures defined in the EC guidelines and adapted to the Spanish context. The MA considered this as particularly important and relevant, especially given the lack of national fraud-prevention legislation. The fact that IBs function with a high degree of autonomy and are thus difficult to monitor and control is another reason for creating this overview of function and procedures.

Practice 7 – Cooperative approaches to conducting the FRA

Case study: Spain – Coordinated approach to create a compendium of anti-fraud procedures of the MA, CA and IBs

Process

The entire process for developing the MA and CA Blue Book and the individual IBs' Blue Books took one year.

Structure

Ten high-level and experienced MA staff members were responsible for supervising the work of IBs and ensuring that it was in line with the Blue Book prepared by the MA. An experienced staff member of the AA and the Spanish AFCOS were also involved in the process, mainly reviewing and verifying the compliance of the procedures proposed by IBs, and of the tailored anti-fraud measures proposed. The AA and AFCOS also regularly provided advice and suggestions.

Steps

The MA and CA started with creating their own Blue Book and devising the methodology for conducting the FRA. Since this was the basis for the IBs' work, the MA had to ensure that it correctly understood the concept and methodology of the FRA devised by the EC, and that the topics to be covered in the Blue Books included all those suggested by the EC.

Once this **preparatory work** was completed, the MA provided IBs with a copy of its Blue Book, a template thereof, the EC's FRA template and its guidance note. The MA then **put in place an assistance and communication plan for IBs,** including training sessions and workshops, in order to provide IBs with a place to share their feedback and concerns and ask questions related to the tasks assigned to them. IBs have attended **more than 25 training sessions** to show them the structure and methodology used by the MA to create its Blue Book, which should be the basis of their work.

As part of the training sessions, **the MA gave presentations** to IBs, providing an overview of the legal framework for the 2014-2020 programming period, and specifically the legal basis for drafting MCS and for conducting an FRA. These training sessions were very practical as they also aimed to explain in more detail the structure of the FRA template and the steps to fill it in, using screenshots of the tool. A detailed explanation was also provided of the methodology for assessing the impact and likelihood of risks before and after putting in place the control measures. The list of mitigating measures prepared by the EC was also discussed, and practical exercises to tailor those measures to the specific context of IBs were explored.

Following these training sessions, **six experimental trials were conducted with six IBs over a period of 3 months.** The rationale of the MA for conducting experimental trials was to make sure the assistance and communication campaign was successful, and that IBs had sufficient knowledge and confidence to start work on both the individual Blue Books and the FRA. The trial was an **iterative process**, during which the MA, CA, AA and AFCOS were regularly reviewing the work of IBs and providing comments and suggestions for improvement. The first versions of the Blue Books and FRA received by the MA were very poor and the majority of the IBs had to edit them at least twice or more before they were deemed satisfactory.

The last part of the experimental trial involved the six IBs **actually implementing the procedures** described in their individual Blue Books, as well as the customised anti-fraud measure they had devised.

Once the six experimental trials were deemed satisfactory by the MA, the same approach was rolled out with all the remaining IBs under the supervision of the MA controlling department. By Q4 2018, IBs were still in the process of testing these procedures and anti-fraud measures, following which they will create a new appendix to the Blue Book in case of any amendments.

Practice 7 – Cooperative approaches to conducting the FRA

Case study: Spain – Coordinated approach to create a compendium of anti-fraud procedures of the MA, CA and IBs

Expected results

The process of creating a Blue Book and having a FRA conducted by each IB was a success. Indeed, 100% of the IBs followed the Blue Book template and successfully prepared their FRA. Feedback provided by IBs during this process was positive as the majority of them found that having all the procedures clearly explained was key to the sound financial management of the OPs. Another tangible benefit was that staff members responsible for conducting the procedures now tend to be more accountable for their work and have a clear vision of their role and responsibilities, which is crucial to the fight against fraud and corruption.

Although it is still early to draw conclusions on specific benefits gained from this cooperation process, the authorities are already noticing increased efficiency in the procedures implemented, thus allowing staff members performing administrative and on-the-spot verifications to be more cautious and attentive to fraud and corruption risks. Furthermore, this cooperation seems to result in positive benefits to the reputation of the MA and the IBs, there appears to be fewer errors and irregularities and fewer complaints from beneficiaries or applicants.

Finally, this process was a win-win for the MA and IBs as they both stated that they had learnt a lot about their work and each other, and had improved their knowledge and capacity on preventing and detecting fraud and corruption.

Lessons learned

In addition to drawing some preliminary benefits from this exercise, the MA also learns some lessons from it. One takeaway is that although the process for conducting the work was very time-consuming and challenging, especially the part regarding the FRA, it is the only way that all the parties involved are able to learn about fraud prevention and improve their capacities therein.

Another takeaway is that, when using EC templates, it is crucial to adapt them to the MA's or IB's specific aspects to ensure that staff members take them on board and use them properly. With regard to the FRA, it was deemed useful but it appears that extensive explanations need to be provided before fully understanding the concept and methodology. The involvement of all parties participating in programming, managing and controlling the OPs, and especially the involvement of top management, is key to ensure consensus when defining and implementing the most effective and proportionate anti-fraud measures used.

Finally, when conducting educative training and workshops, promoting best practices and practical examples is important because it is also during these activities that new good practices are unveiled.

Contact details

Name of the entity: Ministry of Finance, Directorate-General for European Funds

Website: http://www.sepg.pap.hacienda.gob.es/

E-mail: fondoscomunitarios@sepg.minhafp.es

Practice 8 – Fostering an anti-fraud culture

Summary of the practice

An anti-fraud culture is a fundamental part of a comprehensive anti-fraud system. Anti-fraud culture includes a number of elements that form intolerance and unacceptance of fraud in the organisation and in society.

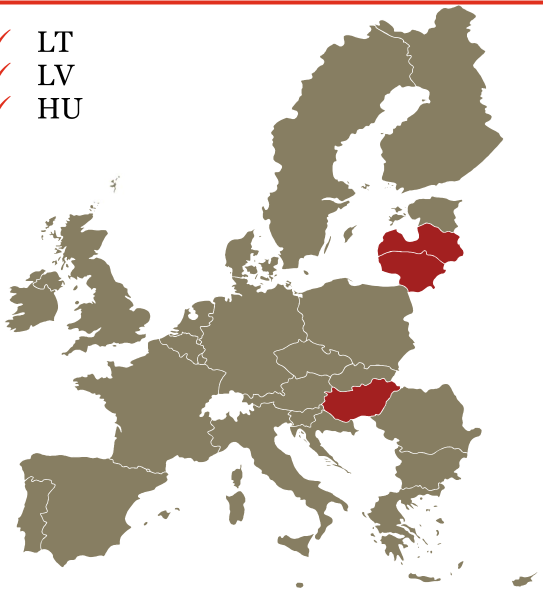
The anti-fraud practices that focus on building a strong anti-fraud culture may include organisation-related activities and awareness-raising campaigns for the general public. The first group of practices includes tone from the top and the availability of a code of ethics, while also featuring the elements of fraud awareness in employees' job descriptions. When applying practices to the general public, they take the role of regional or national initiatives on fraud intolerance or increased transparency.

Fostering an anti-fraud culture aims at increasing public awareness of fraud risk and mitigating tools, uniting them in the fight against corruption and fraud, and making society more involved in anti-fraud activities.

Most of the MAs in the sample have implemented some of the elements of anti-fraud culture in their organisations, albeit within the limits of necessary procedures. The practices featured below are recognised initiatives at national level aiming at improving general anti-fraud awareness.

Practice spotted in...

- ✓ LT
- ✓ LV
- ✓ HU



Expected impact on the anti-fraud system

Awareness-raising

Activities aiming at improving anti-fraud culture generally increase awareness of fraud issues among the target audience. When implemented within an organisation, these measures reinforce the message of management's commitment to fighting fraud and employees' responsibility to behave ethically. When used as a part of wider regional or national initiatives, they are used to create the mass movement of fraud and corruption intolerance using common logos or branding. Overall, such practices reinforce the understanding of fraud risks and create a culture of unacceptance and resistance in society.

Preventing fraudulent activities

The systematic implementation of measures focusing at an anti-fraud culture has a positive effect on fraud prevention. Thus, creating an environment that is sensitive to corruption and fraud suggests that more attention will be paid to the risk of fraud and its prevention in organisations and among the public. The long-term impact of the growing anti-fraud culture lies in the strong commitment to prevent and report any suspicious or fraudulent activities, as well as improving the transparency of processes and budget management at all stages of the project cycle.

*This anti-fraud practice is considered a **soft prevention measure** designed to reinforce fraud prevention and strengthen the anti-fraud environment and ethical culture. Implementing activities related to the anti-fraud culture have a horizontal impact and touch upon all fraud risks.*

Practice 8 – Fostering an anti-fraud culture

Examples of the practice

Latvia – #FraudOff awareness-raising campaign

How it works

To combine efforts in the fight against the shadow economy, corruption and other fraudulent activities affecting the state budget and overall social welfare, the Latvian Government has implemented a social information campaign known as the anti-fraud movement – #FraudOff! The long-term goal of the movement is for Latvian society to have zero tolerance of fraud.

The idea of the campaign is based on the combined efforts of public institutions, businesspeople, social partners and everyone in society in the fight against fraud. The campaign focuses on preventive measures, including promoting public awareness of the shadow economy and fraud, and their negative consequences for each individual and the country's general prosperity. In addition, the campaign explains how to report fraud to the relevant law enforcement authorities if someone suspects or knows about a specific case of fraudulent activity.

Unique features

#FraudOff! is the first initiative of its kind in Latvia, bringing together more than 20 public institutions and partners in a joint anti-fraud campaign.

The main partners in the initiative are ministries and State authorities, e.g. the Ministry of Finance, the Ministry of the Interior, the Ministry of Economics, the State Revenue Service, the State Police, the Corruption Prevention and Combating Bureau, the Competition Council, the Procurement Monitoring Bureau and others, as well as Transparency International Latvia.

The anti-fraud movement brings together private organisations that are ready to join hands to fight against fraud and involve all of Latvian society in this fight. In 2018, #FraudOff initiative has additionally been supported by Latvian law enforcement authorities, combining efforts in the fight against fraud with promoting education among society.

#FraudOff! has a dedicated website (http://atkrapies.lv/), which contains a message on the goals of the initiative, information on the level of fraud and corruption in Latvia, and practical advice to the public on the areas sensitive to fraud in day-to-day life:

- What you should know when entering into an employment contract with a potential employer;
- How to check whether your employer is paying tax;
- What occupational safety regulations you should consider;
- How to recognise a fake branded product;
- How to recognise fake money;
- What you should know about food labelling.

In 2018, the #FraudOff! movement is specifically addressing people aged 16 to 24, informing them of fraud risks and what they should consider when entering into an employment relationship with a potential employer.

All Latvian citizens, businesses and organisations are invited to participate in the anti-fraud movement. #FraudOff!'s main tool is the use of its logo by public and private institutions. Supporters of the movement are invited to use the campaign brand in everyday communication. On the movement's website, it is possible to download campaign posters, visual materials for websites and social networks, as well as to apply for a special sticker that can be placed on doors at a company, institution or shop. Citizens are also encouraged to use the hashtags #atkrāpies! and #fraudoff!, as well as #viltotaiszaķis, which translates as #fakechick. The organisers emphasise that the movement's brand will not serve as a quality mark, but rather will demonstrate an organisation or person's negative attitude towards fraudulent activities. For traders, it is also an opportunity to show that they sell original products and not counterfeit ones.

Expected impact

The #FraudOff! movement has been considered a success in Latvia and abroad. It was honoured at the IPRA Golden World Awards 2018 for the best concept and communication campaign. #FraudOff! has been successful in uniting public authorities, entrepreneurs, social partners and everyone in society in combating fraud. It has also successfully raised public awareness of the shadow economy and fraud, and their negative consequences for each individual and the economy in general.

Lithuania – "Jonvabaliai" transparency initiative

How it works

"Jonvabaliai" ("Fireflies") is the first voluntary initiative in the EU to encourage project promoters to be more open to the public and to seek greater transparency for themselves. EU project promoters from this initiative now report not only to various institutions, but also to the **general public**, and **each resident of Lithuania** can be sure that funds are invested and managed transparently**.**

Jonvabaliai was created by eight Lithuanian public organisations (including the Ministry of Finance and Transparency International Lithuania) with the support of the European Social Fund. Total investment for the "Transparency Initiative Jonvabaliai" project is EUR 58,873, with the European Social Fund contributing EUR 50,042 through the "Technical Assistance" Operational Programme for the 2007-2013 programming period.

The goal of the initiative is to encourage enterprises, institutions and organisations to share information on the use of EU funds and to improve transparency-budget spending for EU-funded projects. The initiative also aims to provide the public with more information on EU investments from the project promoters and to encourage joint efforts to achieve positive systemic changes in the area of transparency.

The main objectives of the initiative are:

- to seek greater transparency in the implementation and payment of EU-funded projects;
- to encourage project promoters to operate on the principles of integrity and openness and to make changes in the field of transparency;
- to rate project promoters according to the transparency of the use and settlement of investments, giving them a bonus (from 1 to 3);
- to present good examples of EU investment; and
- to increase public awareness of the use of EU funds in Lithuania.

Jonvabaliai is implemented in the form of an online platform that collects information on the projects funded by the EU and shares this information with the public.

Unique features

The Jonvabaliai online platform (www.jonvabaliai.lt) provides information on projects funded by the EU. More specifically, the platform and maps specify the location of each project and explain what the project does, how much money it has received, and how this money is managed. Via a website, project managers can voluntarily submit information about project results, prices, public procurements, stakeholders, risk-management practices, etc.

The more information a project shares, the more "fireflies" it earns. **One firefly** given to a project means that the project is dedicated to improving transparency, while **three fireflies** represent the highest level of transparency and openness to the public.

When a user visits the website, they see a map highlighting all EU-financed projects, with each project's number of fireflies being fully visible – giving them a clear visual understanding of how transparent a project is.

Practice 8 – Fostering an anti-fraud culture

Members of the Jonvabaliai Initiative have the right to use the logo of the initiative to demonstrate that their EU-funded project provides detailed information contributing to the use of responsible EU funds.

Expected impact

Since the start of the project in September 2014, more than 630 project managers have joined the initiative following a series of awareness-raising campaigns. These included an advertising campaign, a contest for municipalities, the possibility to use the initiative's logo, invitations to attend open days for projects, the production of road signs inviting people to visit the projects, and a TV show dedicated to the Fireflies project.

During the two-year implementation of the project, the Jonvabaliai platform was visited by 35,500 unique visitors, accounting for 140,000 page views. Following the project's implementation, 62% of Lithuanian citizens think they have enough information on EU funding and 51% think the money is managed transparently – nearly twice as many people as before the Fireflies initiative.

The success of the initiative is recognised at EU level. In 2016, the Jonvabaliai initiative was honoured at the prestigious RegioStars Awards in Category 5 ("Effective Management") as the best regional transparency initiative.

KN-01-19-673-EN-N

Publications Office

doi: 10.2776/488340