MINISTRY OF FINANCE

PUBLIC INTERNAL FINANCIAL CONTROL DEPARTMENT

GUIDELINES
FOR RISK MANAGEMENT OF FRAUD AND CORRUPTION

Skopje, June 2017

EXECUTIVE SUMMARY

The purpose of these guidelines is to assist and make recommendations on the public sector entities to take effective and proportionate action against irregularities and fraud (including corruption), taking into account the risks identified[1] in order to protect the Budget of the Republic of Macedonia, EU funds and funds from other domestic and foreign sources. These guidelines also provide a list of schemes of fraud and appropriate indicators of fraud that may be relevant to raise awareness of fraud, so that the management and control systems can be effectively enhanced in the area of prevention and detection of fraud .

The public sector entities should take a proactive, structured and targeted approach to managing the risk of fraud and take proactive and proportionate measures to combat fraud by cost-effective means. Therefore, it is taking a stance of zero tolerance for fraud, starting with the acceptance of the same from the top of management.

Good risk assesstment of fraud, combined with the clear highlight commitment to fighting fraud, it can send a clear message to potential perpetrators of fraud. Established effective sound control systems can significantly reduce the risk of fraud, but can not completely eliminate the risk of fraud or its disclosure. The systems also must ensure the establishment of procedures for detecting fraud and taking appropriate measures in case of detection of suspected fraud.

These guidelines should become a guide through the steps to remove all remaining cases of fraud by establishing a sound financial management measures and their effective implementation. However, the general objective of effectively managing the risk of fraud and implementation of effective and proportionate measures to combat fraud, which in practice means targeted and differentiated approach for each program and condition.

Therefore, the tool for self assessment of the risk of fraud, which is attached to these guidelines, along with more detailed instructions, can be used to estimate the impact and likelihood of occurrence of the usual risks of fraud. Furthermore, the guidelines specified recommended mitigation controls that can contribute to further reduce the remaining risks that are not efficiently removed by existing controls. Operational objective of the management body should be providing answers to frauds that are proportionate to the risks and adapted to the specific conditions associated with the management of funds earmarked for a particular program or region.

After the risk assessment and the establishment of related controls for mitigation on public sector entities are recommended certain conditions to be addressed by establishing concrete indications of fraud (warning signs) and ensure effective cooperation and coordination between public sector entities, audit services and the public prosecutor's office as an investigative body. In this, too, it is advisable and using tools (IT program) to measure specific risks, which can help in the identification, prevention and detection of risky operations, projects, customers and contracts / contractors, and also It serves as a preventive instrument.

The fraud risk self-assessment[2] is clear, logical and practical and is based on five main methodological steps:

1. Quantification of the risk that a given fraud type would occur by assessing impact and likelihood (gross risk).

2. Assessment of the effectiveness of the current controls in place to mitigate the gross risk.

3. Assessment of the net risk after taking into account the effect of any current controls and their effectiveness i.e. the situation as it is at the current time (residual risk).

[1] Article 50 of the Law on Public Internal Financial Control ("Official Gazette" no. 90/2009, 188/2013 and 192/2015)

[2] That is proposed and by the European Commission

4. Assessment of the effect of the planned mitigating controls on the net (residual) risk.

5. Defining the target risk, i e the risk level which the management body considers tolerable after all controls are in place and effective.

1. INTRODUCTION

1.1. Context

Budget users are responsible for the planning and execution of the budget, in accordance with the principles of comprehensiveness, specificity, economy, efficiency, effectiveness, transparency and sound financial management[3], which implies the execution of the budget in accordance with effective and efficient internal control as a process applicable at all levels of funds management.

The establishment of management and control is performed in accordance with regulations harmonized with the EU legislation, under which is necessary to constantly confirm whether the systems function effectively by conducting audits to prevent, detect and correct irregularities and fraud.

In the case of irregularity or suspected fraud or corruption, the person responsible for irregularities in the management body is obliged to take the necessary measures and inform the Public Prosecutor of the Republic of Macedonia, the Ministry of Finance - Financial Police Office (AFCOS[4]) and Department for Financial Inspection in the Public Sector, and within 15 days for taken measures in writing, to inform the person who reported the irregularities or fraud, except in the case of an anonymous report. In this, the staff including internal auditors that reported irregularities or suspected fraud shall be provided the protection of identity and acquired labor rights based on law.

European Commission asking to be informed of irregularities concerning the cases related to the use of IPA funds, regardless of whether the abnormality is unintentional or intentional (ie fraud), and the costs that this has an impact must be excluded from co -finansing from the EU budget.

Hence the need for public sector entities to introduce **effective and proportional measures against fraud and corruption, taking into account the identified risks**. The public sector entities are responsible to show that attempted fraud is unacceptable and will not be tolerated. Tackling fraud, its causes and consequences is a major challenge for any public institution, because fraud is devised in such a way to avoid being discovered. The public sector entities are advised, in assessing the extent to which it can be assumed that the overall environment is exposed to potential corruption and fraud, to take into account the index of perception of corruption organization Transparency International[5] reports on EU anti against fraud.[6]

The possibility of fraud must not be neglected and should be viewed as a set of risks that need to be managed together with other operating risks or potential negative events. Therefore the assessment of the risk of fraud can be implemented using the existing principles and tools for risk management. By effectively established a sound system of control can reduce the risk of fraud or non-disclosure, but can not eliminate the likelihood of its occurrence. The general goal should be the removal of the main risks of fraud to the desired manner, taking into account that in addition to the basic requirements for the general benefit of all additional measures to combat fraud should exceed the total cost of taking these measures (principle of proportionality) taking into account the great impact of fraud and corruption on reputation.

[3] Article 37 of the Budget Law published in the "Official Gazette" no. 64/2005; 4/2008; 103/2008; 156/2009, 95/2010; 180/2011; 171/2012 and 192/2015)

[4] Organizational unit to prevent irregularities and fraud (Anti-Fraud Coordinating Structures - AFCOS)

[5] http://cpi.transparency.org/cpi2012

[6] Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee of 6 June 2011 – Fighting corruption in the EU (COM (2011) 308 final).

In order to assess the impact and likelihood of potential risks of fraud that could harm the financial interests are advised public sector entities to use **the tool to assess the risk** of fraud given in **Annex 1**.

Annex 2: **Exposure to the risk of fraud**, an example that can be used as a tool that shows the types of fraud that can occur in an organization. Annex can serve as a starting point for determining the areas that are susceptible to fraud.

The assessment should be conducted by a team of self-assessment, which determines the management body. The list of **recommended but non-binding controls** to mitigate that the management body may be established in response to residual risks are found in **Annex 3**. The appropriate measures should contribute to further mitigate the remaining risks determined by self-assessment, but have not yet effectively removed with existing controls.

Furthermore, in **Annex 4** is proposed non-binding form of **policy statement to combat fraud** for those public sector entities who want their program to combat fraud to express in the form of a statement of policy.

In addition to these guidelines, provide **guidance and audit services** to check the activities that public sector entities have conducted assessments of the risk of fraud and appropriate measures to reduce the risk of fraud. Checklists in **Annex 5** could prove useful for the revision of the systems that are implement the audit services.

Annex 6 shows the **red flags of behavior that reveal the perpetrators of fraud**. They show certain traits of behavior which represents an indicator of fraudulent behavior that can improve our ability to detect fraud.

In **Annex 7** is presented a list of sixteen common and recurrent fraud schemes with description of the scheme and the relevant fraud indicators (red flags) in contracts and procurement area.

In **Annex 8** is presented a list of sixteen common and recurrent fraud schemes with description of the scheme and the relevant fraud indicators (red flags) in the area of fraud in labor costs and consulting services.

1.2. A proactive, structured and targeted approach to managing the fraud risk

The attached practical fraud risk self-assessment tool targets the main situations where key processes in the implementation of the programmes could be most open to manipulation by fraudulent individuals or organisations, including organised crime, the assessment of how likely and how serious these situations could be and, what is currently management body being done by the management body to tackle them. Three selected key processes considered to be most exposed to specific fraud risks should be targeted:

- selection of applicants;
- implementation and verification of the operations;
- certification and payments.

The end output of the fraud risk assessment should be the identification of those specific risks where the self-assessment concludes that not enough is currently being done to reduce the likelihood or impact of the potentially fraudulent activity to an acceptable level. This assessment will then form the basis for responding to the deficiencies by choosing effective and proportionate anti-fraud measures from the list of recommended mitigating controls. In some cases, the conclusion could be that most residual risks have been addressed and that therefore very few, if any, additional anti-fraud measures are required. In all assessment scenarios, it would be expected that arguments can be provided by the management body to support its conclusions.

2. DEFINITIONS

This risk assessment deals only with specific fraud risks, not irregularities. **However, indirectly, effective implementation of the exercise may also have an impact on prevention and detection of irregularities at large**, being understood as a larger category than fraud.

It is the element of intention which distinguishes fraud from irregularity.[7]

2.1. Definition of irregularity

According to Decree on the procedure for preventing irregularities, the way of cooperation, form, content, deadlines and manner of reporting irregularities, adopted by the Government of the Republic of Macedonia[8]:

"Irregularity is non-compliance or incorrect application of laws and regulations and international agreements, resulting from work or omissions of the beneficiaries of public funds, which have or could have a detrimental impact on the State Budget, EU funds and funds other domestic and foreign sources, whether it is revenue / income, expenditures / expenses, returns, inheritances or obligations "

2.2. Definition of fraud

According to Decree on the procedure for preventing irregularities, the way of cooperation, form, content, deadlines and manner of reporting irregularities, adopted by the Government of the Republic of Macedonia:

"Fraud is any **intentional** act or omission relating to: the use or presentation of false, incorrect or incomplete statements / reports or documents that resulted misappropriation or wrongful retention of public funds, EU funds and funds from other domestic and foreign sources ; disclosure of information, thus breaking any specific obligation with the same effect and misuse of such funds for purposes other than those for which the funds were originally allocated. "

2.3. Definition of corruption

According to the Law on Prevention of Corruption[9] "Under corruption Is implied using of function, public authorization, official duty and position to achieve any benefit for himself or another." The broader definition of corruption used by the European Commission is abuse (public) position for private benefit. With Corrupt payments facilitate many other types of fraud, such as issuing false invoices, false charges or delinquency rates of the contract. The most common forms of corruption are corrupt payments or other benefits in that the receiver (passive corruption) receiving bribes from the provider (active corruption) in exchange for service.

3. FRAUD RISK SELF-ASSESSMENT

3.1. The tool

The main objective of the fraud risk assessment tool at Annex 1 is the facilitation of a self-assessment by the management body of the impact and likelihood of specific fraud scenarios occurring. The specific fraud risks which should be assessed were identified through knowledge of previous fraudulent cases encountered in cohesion policy, as well as commonly recognised and recurring fraud schemes.

[7] The reasons behind fraudulent behaviour have been dealt with in COCOF 09/0003/00 of 18.2.2009 - Information Note on Fraud Indicators for ERDF, ESF and CF.

[8] "Official Gazette of Republic of Macedonia" no. 63/2011

[9] ("Official Gazette of Republic of Macedonia " no. 28/2002, 46/2004, 126/2006, 10/2008, 161/2008, 145/2010, 97/2015 and 148/2015)

In other words, the tool has been pre-populated with a set of recognised specific risks.

Any other known risks for the specific programme / region under assessment should be added by the self-assessment team (see section 3.2. below).

The guidance in Annex 1 explains in detail how to complete the fraud risk assessment tool.

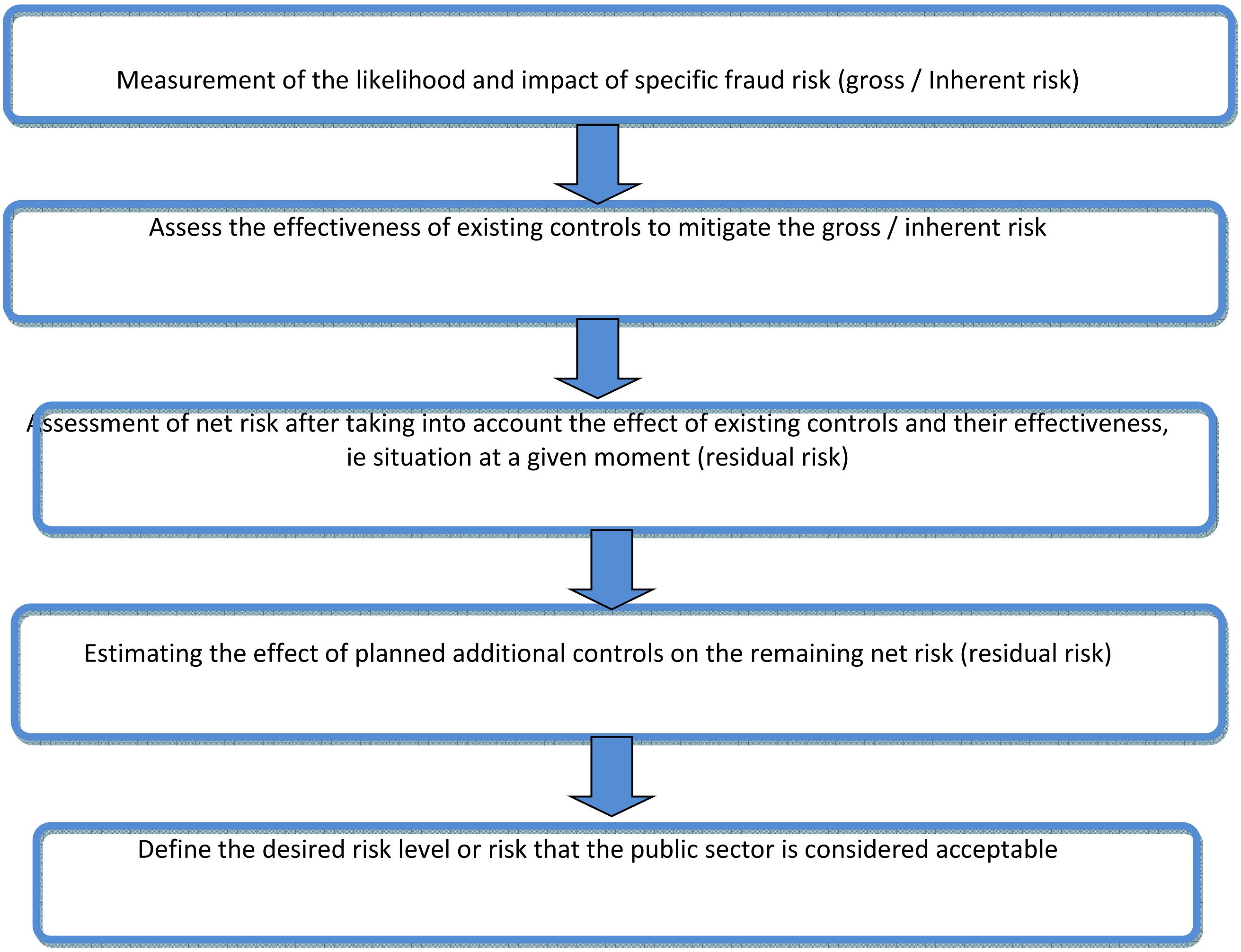
The tool covers the likelihood and impact of specific and commonly recognised fraud risks particularly relevant to the key processes:

- selection of applicants (worksheet 1 of the spreadsheet);
- implementation of the projects by the beneficiaries, focusing on public procurement and labour costs (worksheet 2);
- certification of costs by the management body and payments (worksheet 3).

Each section is preceded by a cover sheet, which lists the specific risks relevant to the section.

Moreover, the management body is recommended to assess fraud risks in relation to any public procurement it manages directly, e.g. in the context of technical assistance (worksheet 4). In case the management body does not carry out any public procurement for which a fraud risk assessment is necessitated, section 4 need not be filled in.

The methodology for this fraud risk assessment has five main steps:


Measurement of the likelihood and impact of specific fraud risk (gross / Inherent risk)
Assess the effectiveness of existing controls to mitigate the gross / inherent risk
Assessment of net risk after taking into account the effect of existing controls and their effectiveness, ie situation at a given moment (residual risk)
Estimating the effect of planned additional controls on the remaining net risk (residual risk)
Define the desired risk level or risk that the public sector is considered acceptable

For each of the specific risks, the overall objective is to assess the ‘gross’ risk of particular fraud scenarios occurring, and then to identify and assess the effectiveness of controls already in place to mitigate against these fraud risks either from occurring or ensuring that they do not remain undetected. The result will be a "net" existing risk[10] based on which, in the event of significant or critical residual risk should be adopted an internal action plan aimed at improving control and further reduce the exposure of the public sector to negative consequences (i.e.establishment of additional effective and proportionate measures to combat fraud, if necessary - see list of recommended mitigation controls[11] in Annex 3).

3.2. Composition of the self-assessment team

Depending on the size of the programme and of the public sector entity, it may be that each of the implementation processes are executed by different departments within the public sector entity, and it is essential that the most relevant actors take part in the assessment in order that it is as honest and accurate as possible and so that it can be done in an efficient and smooth way. The assessment team could therefore include staff from different departments of the management body having different responsibilities, including selection of operations, desk and on the spot verification and authorisation of payments, as well as representatives from the certifying authority and implementing bodies. Management body may want to consider involving the Anti-Fraud Coordination Services ('AFCOS') or

[10] See Annex 2, Exposure to the risk of fraud - The types of fraud that can appear

[11] It is composed of non-binding proposals for additional controls to further mitigate the residual risk.

other specialised bodies, which could bring in specific anti-fraud expertise into the assessment process. As the audit authority will audit the completed risk assessment, it is recommended that it does not take a direct role in deciding on the level of risk exposure, but it could be envisaged to participate in the assessment process in an advisory role or as an observer.

For obvious reasons, the self-assessment should not be outsourced as it requires a good knowledge of the operating management and control system and the programmes's beneficiaries.

3.3. Frequency of the self-assessment

The recommendation is that this tool should be completed in full on an annual basis, as a general rule, or every second year. However, more regular reviews of progress against action plans related to additional controls which were put in place, changes to the risk environment and the continuing adequacy of assessment scores may be necessary (e.g. through management meetings). When the level of risks identified is very low and no instances of fraud were reported during the previous year, the MA may decide to review its self-assessment only each second year. The occurrence of any new fraud instance, or main changes in procedures and/or staff, should immediately lead to a review of perceived weaknesses in the system and of relevant parts of the self-assessment.

As the internal audit will audit the completed risk assessment, it is recommended that it does not take a direct role in deciding on the level of risk exposure, but it could be envisaged to participate in the assessment process in an advisory role or as an observer.

For obvious reasons, the self-assessment should not be outsourced as it requires a good knowledge of the operating management and control system and the programmes's beneficiaries.

4. GUIDANCE ON MINIMUM REQUIREMENTS FOR EFFECTIVE AND PROPORTIONATE

ANTI-FRAUD MEASURES

Whereas this section provides general guidance on principles and methods which should be employed by the management body to combat fraud, **Annex 3** provides for each specific risk identified in the fraud risk assessment, the recommended mitigating controls which could be put in place in order to seek to reduce the risks to an acceptable level.

The minimum standards set out in this chapter by which management body are recommended to comply with relate to the anti-fraud cycle.

In order to successfully tackle the issue of fraud, the management body should develop a structured approach to tackling fraud. There are four key elements in the anti-fraud cycle: prevention, detection, correction and prosecution.

The combination of a thorough fraud risk assessment, adequate preventative and detective measures, as well as coordinated and timely investigations by competent bodies could significantly reduce the fraud risk as well as provide adequate deterrence against fraud.

4.1. Anti-fraud policy

Many organisations use an anti-fraud policy to communicate their determination to combat and address fraud. Within any such policy, which should be simple and focused, the following topics should be covered:

- Strategies for the development of an anti-fraud culture;
- Allocation of responsibilities for tackling fraud;
- Reporting mechanisms for suspicions of fraud;
- Cooperation between the different actors.

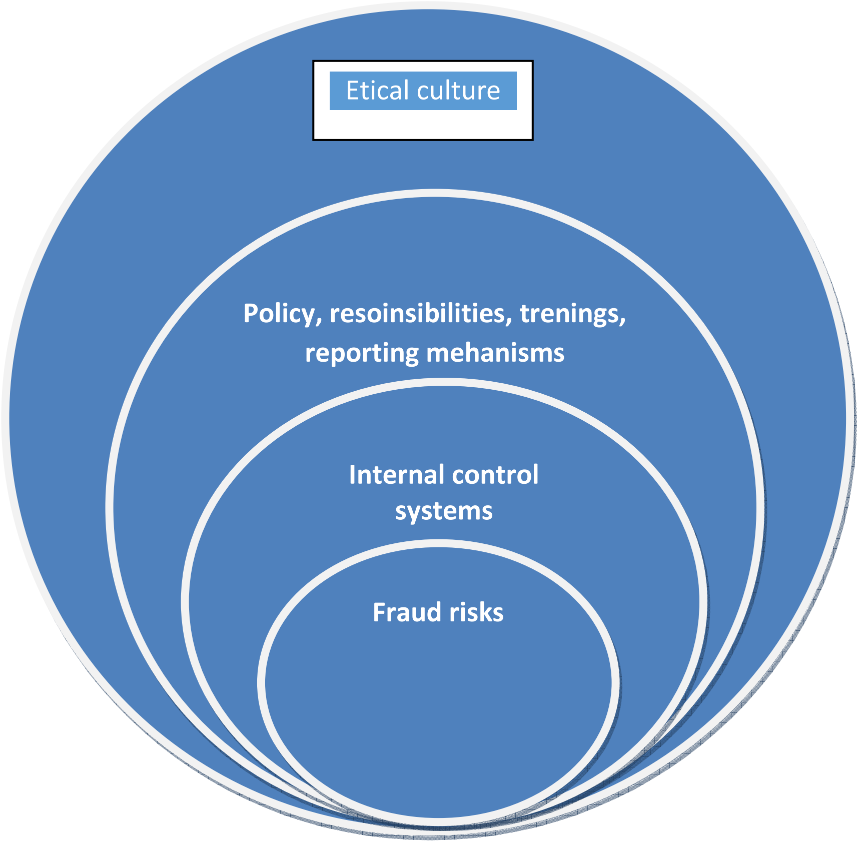
This policy should be visible within an organisation (distributed to all new staff, included on intranet) and it should be clear to staff that it is actively implemented, via avenues such as regular updates on fraud matters and reporting of outcomes of investigations into fraud. See the suggested template for an anti-fraud policy at **Annex 4**, which provides a voluntary template for an anti-fraud policy statement for the benefit of those public sector entities which wish to go beyond the immediate regulatory requirements and to formalise and communicate internally and externally their official position with regard to fraud and corruption.

4.2. Prevention

If the management body demonstrates a clear commitment to combat fraud and corruption, raises awareness about its preventative and detective controls, and is determined in transmitting cases to the competent authorities for investigations and sanctions, it will send a clear message to any potential perpetrators and could change behaviours and attitudes towards fraud.

Given the difficulties in proving fraudulent behaviour and repairing reputational damage, it is generally preferable to prevent fraudulent activity rather than to have to deal with it after the event. Prevention techniques most often revolve around reducing opportunities to commit fraud via the implementation of a robust internal control system, combined with a proactive, structured and targeted fraud risk assessment, but comprehensive training and awareness raising activities and the development of an **'ethical' culture** can also be used to combat any potential 'rationalisation' of fraudulent behaviour.

The strongest preventative defence against fraud is the operation of a robust system of internal control which should be designed and operated as a proportionate response to the risks identified during a risk assessment exercise. An organisation should however also work to create the right structures and culture to discourage potential fraudulent behaviour.


Etical culture
Policy, resoinsibilities, trenings, reporting mehanisms
Internal control systems
Fraud risks

4.2.1. Ethical culture

The creation of an anti-fraud culture is key both in deterring potential fraudsters and also in maximising the commitment of staff to combat fraud within the public sector entity. This culture can be created by a combination of specific antifraud structures and policies, as shown in the second circle in the above diagram and discussed in more detail below, but also through the operation of more general mechanisms and behaviours:

- **Mission statement** – a clear expression, visible to all internal and external observers, that the management body is striving to achieve the highest ethical standards;
- **Tone from the top** – oral and/or written communication from the highest level of the management body that the highest standard of ethical behaviour is expected from staff and beneficiaries (the latter can be implemented through the grant letters and contracts);
- **Code of conduct** – a unambiguous code of ethics that all staff must routinely declare adherence to, covering such things as:
  - Conflicts of interest – explanation and requirements and procedures for declaring them;
  - Gifts and hospitality policy – explanation and responsibilities of staff for compliance;
  - Confidential information – explanation and responsibilities of staff;
  - Requirements for reporting suspected fraud or breaches of the Code.

In short, staff must comply with principles such as integrity, objectivity, accountability and honesty.

4.2.2. Allocation of responsibilities

Within the public sector entity, there should be a clear allocation of responsibilities for setting up management and control systems which comply with EU requirements and for verifying that these systems function effectively in preventing, detecting and correcting fraud. This is to ensure that all actors fully understand their responsibilities and obligations, and to communicate both internally and externally, towards all potential programme beneficiaries, that the organisation has a coordinated approach towards combatting fraud.

4.2.3. Training and awareness raising

Formal training and awareness-raising can be included within the organisation’s overall risk management strategy, as necessary. All staff could be trained on both theoretical and practical matters, both to raise awareness of the public sector entity's anti-fraud culture and also to assist them in identifying and responding to suspected instances of fraud. It should cover the detail of any anti-fraud policy, specific roles and responsibilities and reporting mechanisms.

Awareness-raising can also be carried out via less formal avenues, such as through newsletters, posters, intranet sites or inclusion as a regular agenda item for group meetings.

4.2.4. Internal control systems

The strongest defence against potential fraud is a well-designed and operated system of internal control, where controls are focused at effectively mitigating the identified risks.

Management verifications must be thorough and the associated on-the-spot controls must be risk-based and carried out with sufficient coverage. **The likelihood of detecting potential fraud cases will increase when management verifications are thorough.** Staff in charge of desk and on the- spot management verifications should be aware of this guidance and guidance for fraud indicators (Annex 6, 7 and 8).

4.2.5. Data analytics and use of special tool

With the growth in sophistication of data gathering, storage and analytics comes an opportunity in the fight against fraud. The analysis of data can significantly improve the process of risk assessment. In this, the data can be compared with data from other organizations in the public or private sector (eg. Tax authorities, government bodies and authorities responsible for checking creditworthiness) and to discover potential high-risk situations.

In the fight against fraud (and irregularities), it is necessary to use tool for in-depth analysis of data in order to identify projects that could be at risk of fraud, conflict of interest and irregularities. It should increase the efficiency of project selection, control on management and audit and further strengthen the identification, prevention and detection of fraud. It should be particularly suitable for identifying and assessing the risks of fraud in the use of IPA funds, including, inter alia, public procurement as an area that is particularly vulnerable to fraud and irregularities, as secret bargaining for tenders.

Proper use of the tool, will be considered as good practice for determining the warning signs and concrete measures to combat fraud and the assessment should be taken into account the adequacy of existing preventive and detective controls. The tool should be introduced gradually in the public sector entities that voluntarily decide to apply for further improving its controls to manage the risk of fraud.

4.3. Detection and reporting

Preventative techniques cannot provide absolute protection against fraud and so the pablic sector management body need systems that detect fraudulent behaviour in a timely manner. Such techniques include analytical procedures to highlight anomalies (e.g. data mining tools), robust reporting mechanisms and ongoing risk assessments.

A strong ethical culture and a sound system of internal control cannot provide absolute protection against perpetrators of fraud. A fraud strategy must therefore take into consideration that instances of fraud may still occur, for which a series of fraud detection measures must be designed and implemented.

4.3.1. Developing an appropriate mindset

The MA could address fraud risks with specialised and focused detection techniques with designated individuals having responsibility for conducting them. In addition to this, all of those involved in implementing a structural funding cycle have a role to play in spotting potentially fraudulent activity and then acting upon it. This necessitates the cultivation of an appropriate mindset. A healthy level of scepticism should be encouraged, together with an up-to-date awareness of what could constitute potential fraud warning signs.

4.3.2. Fraud indicators (red flags)

Fraud indicators are more specific signs or ‘red flags’ that fraudulent activity is taking place, when an immediate response is required to verify whether further action is required.

Indicators can also be specific to those activities frequently taking place under structural funding programmes, such as procurement and labour costs.[12]

These publications should be read in detail and the content widely publicised amongst all staff who are in positions in which they could detect such behaviour. In particular, these indicators must be

[12] For this purpose, the Commission has provided the following information to the Member States: COCOF 09/0003/00 of 18.2.2009 - Information Note on Fraud Indicators for ERDF, ESF and CF, OLAF Compendium of Anonymised Cases – Structural Actions, OLAF Practical guide for conflict of interest and OLAF Practical guide for forged documents.

familiar to all of those working in roles involving the review of beneficiary activities, such as those performing both desk-based and on-the-spot management verifications or other monitoring visits.

4.3.3. Reporting mechanisms

The establishment and promotion of clear reporting mechanisms is a key element of prevention, as well as detection. Any such mechanisms should facilitate the reporting of both suspicions of fraud and also control weaknesses that may increase the MA's susceptibility to fraud. MAs should have clear reporting mechanisms ensuring sufficient coordination on anti-fraud matters with the audit authority and competent investigative authorities, including anti-corruption authorities.

Communication and training with staff about these reporting mechanisms must ensure that they:

- understand where they should report suspicions of fraudulent behaviour or control;
- are confident that these suspicions are acted upon by management;
- are confident that they can report in confidence and that the organisation does not tolerate retaliation against any staff member who reports suspicions.

4.4. Investigation, correction and prosecution

Once a suspicion of fraud has been raised and correctly reported, the MA must transmit the case to the competent authority for investigation and sanctions, including anti-corruption authorities where relevant, and inform OLAF accordingly.

The MA should also conduct a thorough and critical review of any related internal control systems that may have exposed them to the potential or proven fraud.

Once a case of suspected fraud has been detected and reported the competent body has to make an assessment whether an investigation should be opened, recovery and criminal prosecution should ensue, as relevant.

4.4.1. Recovery and criminal prosecution

Recovery of undue payments from beneficiaries is required by MAs and CAs and so they should ensure that they have robust processes in place for following up any potential recoveries of funds spent in a fraudulent manner. These processes should also be clear on the cases in which civil and criminal proceedings will be pursued. The implementation of such sanctions, and the visibility of these, are a key deterrent to potential fraudsters and so the MA should be vigorous in pursuing such outcomes.

4.4.2. Follow-up

Once a fraud investigation has been concluded by competent authorities, or handed over to the relevant authorities for pursuit, a review of any processes, procedures or controls connected to the potential or actual fraud should be conducted. This should be objective and self-critical and should result in clear conclusions about perceived weaknesses and lessons learned, with clear actions, responsible individuals and deadlines. This should also feed into the subsequent review of the self-assessment, as indicated in section 3.3 above.

Full cooperation with investigative, law enforcement or judicial authorities hould be ensured, in particular by keeping files concerning fraud cases in safe places and ensure a proper hand over in case of staff mobility.

5. AUDIT OF RISK ASSESSMENT OF FRAUD AND ANTI-FRAUD MEASURES OF AUDIT UNIT

5.1. A check list of the Audit unit

Draft checklist of audit unit for conducting an audit of the public sector (and its bodies) is in Annex 4. This may be part of a checklist for checking used by audit unit to implement its system audits. The checklist can be used by the independent audit body responsible for assessing the management and control.

5.2. Frequency of the audit verification

In connection with audits on the functioning of the management and control systems, the audit unit should carry out verifications of the effective implementation of the anti-fraud measures by the management as early as possible in the programming period. Depending on the results of such audits and on the identified fraud risk environment, follow-up audits may be carried out as often as necessary. In some cases this may entail annual follow-up audits, depending on the gravity of fraud suspicion for each programme. Here again a targeted and proportionate (riskrelated) approach is recommended. The conclusions should be included in the audit unit annual control report.

The audit unit should also need systematically review the implementation of effective and proportionate anti-fraud measures, as part of its system audits.

Annex 1.

1.1. HOW TO USE TOOL FOR SELF-ASSESSMENT

Tool includes three key actions in three parts:

- selection of candidates / tenderers (1 worksheet spreadsheets)
- The way customers implement projects with an emphasis on public procurement and labor costs (worksheet 2)
- certification / recognition of the costs of the management body and payment (worksheet 3).

Each of the three sections, which contain specific risks that are marked with numbers (eg. RL1, RL2, etc.) precedes front page which contains all the specific risks that are relevant to the case.

In addition, it is recommended that the management body to assess the risks of fraud related to public procurement, which directly manages, for example, in the context of technical assistance (section 4 of the direct public procurement). If the management body does not conduct public procurement which requires an assessment of the risk of fraud, it should not fill section 4.

Note: The team self-evaluation should be completed only shaded squares.

DESCRIPTION OF RISK

For assistance on team, in the tool previously is defined a number of risks. The team should reassess all previously defined risks, but in the case of newly identified risks, it is possible to add more rows.

A complete description of the risk is on the cover (of sections 2 and 4) or specific risk (parts 1 and 3).

Column name	Guides
Reference number of risks	Unique reference number of risks. The letters refer to the part / organisational unit in which the risk is determined (SV = selecting a vendor, IM = implementation and monitoring, CP = confirmation and payment, DPM = direct procurement of management), and the number is ordinal reference. This box should be filled only for newly established risks.
Name of risk	This box should be filled only for newly established risks.
Description of risks	This box should be filled only for newly established risks.
Who is involved in risk?	Details are listed here for entities in which the persons or participants involved in committing fraud, for example, entity, law enforcement bodies, the certifying authority, users and third parties. This box should be filled only for newly

	established risks.
Whether the risk is internal (within the public sector entity), external or the result of a secret agreement?	Details are listed here as to whether fraud is internal (within the public sector entity), external (only one body out of the public sector entity) or the result of secret agreement (between one or more organs). This box should be filled only for newly established risks.

2. Five key steps in the self-assessment

2.1. Gross (inherent) risk

Gross risk refers to the degree of risk, before taking into account the effect of existing or planned controls. Measuring risk usually consists of a combination of "probability" risk - how likely is it that the event will happen "effect / impact" risk - what will be the consequence of the financial and non-financial events. In order to ensure consistency in the assessment, when determining the likely need to set the time frame for implementing the program.

<table>
<tr><th>Column name</th><th>Guides</th></tr>
<tr><td>Effect / impact risk (GROSS)</td><td>Team for risk assessment should choose from the drop down menu impact assessment of the risk of 1 to 4 based on the impact that risk would have had if it showed up, according to the following criteria:
<table>
<tr><th></th><th>Reputation</th><th>Of the goals</th></tr>
<tr><td>1.</td><td>Limited impact</td><td>Additional work for which other processes are delayed</td></tr>
<tr><td>2.</td><td>Small influence</td><td>Delayed fulfillment of the operational objective</td></tr>
<tr><td>3.</td><td>High-impact, eg. because the nature of fraud is particularly serious or covered</td><td>Endangered is achieving operational objective or delayed achieving the strategic goal</td></tr>
</table>
</td></tr>
</table>

<table>
<tr>
<td></td>
<td>
<table>
<tr><td></td><td>several users</td><td></td></tr>
<tr><td>4.</td><td>Official investigation of the party concerned, for example. Parliament and / or negative publicity</td><td>Threatened strategic goal</td></tr>
</table>
</td>
</tr>
<tr>
<td>Probability of risk (GROSS)</td>
<td>
Team for risk assessment should choose from the drop down menu assess the probability of the risk of 1 to 4 based on the impact that risk would have had if it showed up, according to the following criteria:
<table>
<tr><td>1.</td><td>Almost never appeared</td></tr>
<tr><td>2.</td><td>Rarely will appear</td></tr>
<tr><td>3.</td><td>Sometimes will appear</td></tr>
<tr><td>4.</td><td>Often will appear</td></tr>
</table>
</td>
</tr>
<tr>
<td>Overall Risk Assessment (GROSS)</td>
<td>
This square is automatically calculated by multiplying the estimates in the fields of risk impact and likelihood of risk. Are ranked by total score:
<ul>
<li>1-3 - bearable (green)</li>
<li>4-6 - significant (orange)</li>
<li>8-16 - critical (red)</li>
</ul>
</td>
</tr>
</table>

2.2. Existing controls for mitigation

In tool advance is defined a number of proposed preventive controls. These controls are only examples and evaluation team can remove them if the controls do not exist, and it is possible to add more rows in the case of establishing additional controls to prevent identified risk. It is possible the control that is currently assigned to a particular risk is relevant for other risks - in such cases, the controls can couple to repeat. Especially, procedure can be facilitated by simply reference the existing controls that are described and/or mentioned in the description of the management and control system of business processes and manuals.

Column name	Guides
Reference number of control	Sole reference number of the control. The numbers respectively assigned to each risk, for example, control risk KP1 starts by IP1.1 and controlling on risk KR2 starts with IP2.1. This box should be filled only for newly added controls.
Description of control	This box should be filled only for newly added controls.
Do you have evidence of the functioning of this control?	Team for risk assessment should choose from the drop down menu answer "Yes" or "No" to the evidence for the operation of the control. For example, evidence of approval is registered with signature and that the control is visible.
Do you regularly inspecting this control?	Team for risk assessment should choose from the drop down menu answer "Yes" or "No" for regular examination for operation of controls. This can be examined by internal or external audit or other monitoring system.
How much are you sure on the effectiveness of this control?	Partly based on the responses to the previous two questions, the risk assessment team should indicate how confident in the effectiveness of control in terms of mitigation of identified risk (high, medium or low). If control is not substantiated or not tested, the security level will be low. If control is not substantiated, then clearly it will not be possible to investigate.
The effect of combined controls on the effect of risk, taking into account the degree of certainty.	Risk assessment team should choose from the drop down menu score from 1 -4 which indicates their belief that the impact of the risk is reduced with existing controls. The controls that detect scams reduce the effect of fraud because they are proof of the functioning of the mechanisms of internal controls.
The effect of the combined controls the PROBABILITY of risk taking into account the degree of certainty.	Risk assessment team should choose from the drop down menu score from 1 -4 which indicates their belief that the probability of risk is reduced with existing controls. Controls revealing fraud only indirectly reduce the likelihood of fraud.

2.3. Net (residual) risk

Net risk refers to the degree / level of risk after taking into account the impact of existing controls and their effectiveness, ie, the situation at a given moment.

<table>
<tr><th>Column name</th><th>Guides</th></tr>
<tr><td>Effect / impact on the risk (NET)</td><td>This square is automatically calculated by subtracting effect of the combined existing controls to mitigate the risk GROSS effect. Results must be reconsidered based on the following criteria to verify the reasonableness of the assessment:
<table>
<tr><th></th><th>Reputation</th><th>Of the goals</th></tr>
<tr><td>1.</td><td>Limited impact</td><td>Additional work for which other processes are delayed</td></tr>
<tr><td>2.</td><td>Small influence</td><td>Delayed fulfillment of the operational objective</td></tr>
<tr><td>3.</td><td>High-impact, eg. because the nature of fraud is particularly serious or covered several users</td><td>Endangered is achieving operational objective or delayed achieving the strategic goal</td></tr>
<tr><td>4.</td><td>Official investigation of the party concerned, for example. Parliament and / or negative publicity</td><td>Threatened strategic goal</td></tr>
</table>
</td></tr>
</table>

Probability risk (NET)	This square is automatically calculated by subtracting effect of the combined existing controls to mitigate the likelihood GROSS risk. Result must be reconsidered based on the following criteria to verify the reasonableness of the valuation: 1. Almost never appeared 2. Rarely will appear 3. Sometimes will appear 4. Often appears
Overall risk assessment (NET)	This square is automatically calculated by multiplying the numbers in the fields of risk impact and likelihood of risk. Are ranked by total score: • 1-3 - bearable (green) • 4-6 - significant (orange) • 8-16 - critical (red)

2.4. Action plan for the establishment of effective and proportionate measures to prevent fraud

Column name	Guides
Planned additional controls	Here need to give a full description of the planned controls / effective and proportionate measures to prevent fraud. In Annex 3 for each defined risk controls are described recommended control for mitigation.
Responsible person	Here should determine the responsible person (or role) for each planned control. This person should agree to take responsibility for the control and be responsible for the introduction of control and its efficient functioning.
Deadline for implementation	Here is need to specify a deadline for implementation of the new control. The responsible person should be agreed for the period and be responsible for introducing new controls that date.
The effect of combined planned additional controls on **IMPACT** risk	Risk assessment team should choose from the drop down manu score from 1 -4 which indicates

	their belief that the **effect** of the risk is reduced by planned controls.
The effect of combined planned additional controls on the **PROBABILITY** of risk	Risk assessment team should choose from the drop down menu score from 1 -4 which indicates their belief that the **probability** of risk is reduced by planned controls.

2.5. Acceptable risk

The acceptable risk relates to the risk level by taking into account the effect / impact of existing and planned controls.

<table>
<tr><th>Column name</th><th>Guides</th></tr>
<tr><td>Effect / impact on risk (TARGET)</td><td>This square is automatically calculated by subtracting the effect of combined planning controls to mitigate the NET effect of risk. Results must be reconsidered based on the following criteria to verify the reasonableness of the assessment:
<table>
<tr><td></td><td>Reputation</td><td>On the goals</td></tr>
<tr><td>1.</td><td>Limited impact</td><td>Additional work for which other processes are delayed</td></tr>
<tr><td>2.</td><td>Small influence</td><td>Delayed fulfillment of the operational objective</td></tr>
<tr><td>3.</td><td>High-impact, eg. because the nature of fraud is particularly serious or covered several users</td><td>Endangered is achieving operational objective or delayed achieving the strategic goal</td></tr>
<tr><td>4.</td><td>Official investigation of the party concerned, for example. Parliament</td><td>Threatened strategic goal</td></tr>
</table>
</td></tr>
</table>

	and / or negative publicity
Probability risk (TARGET)	This square is automatically calculated by subtracting the effect of combined planning controls to mitigate GROSS probability of risk. Results must be reconsidered based on the following criteria to verify the reasonableness of the assessment: 1. Almost never appeared 2. Rarely will appear 3. Sometimes you appear 4. Often appears
Overall risk assessment (TARGET)	This square is automatically calculated by multiplying the numbers in the fields of risk impact and likelihood of risk. Are ranked by total score: • 1-3 - bearable (green) • 4-6 - significant (orange) • 8-16 - critical (red)

Annex 2

FRAUD RISK EXPOSURES[13]

NOTE: This annex is just an example that can be used as a tool, a reference or starting point. It shows the types of fraud which in an organization can occur. Annex provides a starting point for determining the areas that are susceptible to fraud and to determine specific areas and cultural factors that may affect on the fraudulent behavior.

1) Intentional manipulation of financial statements can lead to:

- a) Inappropriately reported revenues
  - (1) Fictitious revenues
  - (2) Premature revenue recognition
  - (3) Contract revenue and expense recognition
- b) Inappropriately reported expenses
  - (1) Period recognition of expenses
- c) Inappropriately reflected balance sheet amounts, including reserves
  - (1) Improper asset valuation
    - (a) Inventory
    - (b) Accounts receivable
    - (c) Mergers and acquisitions
    - (d) Capitalization of intangible items
  - (2) Misclassification of assets
  - (3) Inappropriate depreciation methods
  - (4) Concealed liabilities and expenses
    - (a) Omission
    - (b) Sales returns and allowances and warranties
    - (c) Capitalization of expenses
    - (d) Tax liability
- d) Inappropriately improved and/or masked disclosures
  - (1) Liabilities omissions
  - (2) Subsequent events
  - (3) Related-party transactions
  - (4) Accounting changes
  - (5) Management frauds uncovered
  - (6) Backdating transactions

[13] The *Fraud Risk Manual* issued by the Association of Certified Fraud Examiners (ACFE), 2007.

e) Concealing misappropriation of assets

f) Concealing unauthorized receipts and expenditures

g) Concealing unauthorized acquisition, disposition, and use of assets

2) Misappropriation of:

a) Tangible assets by

- (1) Cash theft
  - (a) Sales register manipulation
  - (b) Skimming
  - (c) Collection procedures
  - (d) Understated sales
  - (e) Theft of checks received
  - (f) Check for currency substitution
  - (g) Lapping accounts
  - (h) False entries to sales account
  - (i) Inventory padding
  - (j) Theft of cash from register
  - (k) Deposit lapping
  - (l) Deposits in transit
- (2) Fraudulent disbursements
  - (a) False refunds
  - (b) False voids
  - (c) Small disbursements
  - (d) Check tampering
  - (e) Billing schemes
  - (f) Personal purchases with company funds
  - (g) Returning merchandise for cash
- (3) Payroll fraud
  - (a) Ghost employees
  - (b) Falsified hours and salary
  - (c) Commission sales
- (4) Expense reimbursement
  - (a) Mischaracterized expenses
  - (b) Overstated expenses
  - (c) Fictitious expenses
  - (d) Multiple reimbursements
- (5) Loans
  - (a) Loans to nonexistent borrowers
  - (b) Double pledged collateral
  - (c) False application information
  - (d) Construction loans
- (6) Real estate
  - (a) Appraisal value
  - (b) Fraudulent appraisal
- (7) Wire transfer

(a) System password compromise

(b) Forged authorizations

(c) Unauthorized transfer account

(d) ATM

(8) Check and credit card fraud

(a) Counterfeiting checks

(b) Check theft

(c) Stop payment orders

(d) Unauthorized or lost credit cards

(e) Counterfeit credit cards

(f) Mail theft

(9) Insurance fraud

(a) Dividend checks

(b) Settlement checks

(c) Premium

(d) Fictitious payee

(e) Fictitious death claim

(f) Underwriting misrepresentation

(g) Vehicle insurance — staged accidents

(h) Inflated damages

(i) Rental car fraud

(10) Inventory

(a) Misuse of inventory

(b) Theft of inventory

(c) Purchasing and receiving falsification

(d) False shipments

(e) Concealing inventory shrinkage

b) Intangible assets

(1) Theft of intellectual property

(a) Espionage

(b) Loss of information

(c) Spying

(d) Infiltration

(e) Informants

(f) Trash and waste disposal

(g) Surveillance

(2) Customers

(3) Vendors

c) Proprietary business opportunities

3) Corruption including:

a) Bribery and gratuities to

(1) Companies

(2) Private individuals

(3) Public officials

b) Embezzlement

- (1) False accounting entries
- (2) Unauthorized withdrawals
- (3) Unauthorized disbursements
- (4) Paying personal expenses from bank funds
- (5) Unrecorded cash payments
- (6) Theft of physical property
- (7) Moving money from dormant accounts

c) Receipt of bribes, kickbacks, and gratuities

- (1) Bid rigging
- (2) Kickbacks
  - (a) Diverted business to vendors
  - (b) Over billing
- (3) Illegal payments
  - (a) Gifts
  - (b) Travel
  - (c) Entertainment
  - (d) Loans
  - (e) Credit card payments for personal items
  - (f) Transfers for other than fair value
  - (g) Favorable treatment
- (4) Conflicts of interest
  - (a) Purchases
  - (b) Sales
  - (c) Business diversion
  - (d) Resourcing
  - (e) Financial disclosure of interest in vendors
  - (f) Ownership interest in suppliers

d) FCPA violations

- (1) Anti-bribery provisions
- (2) Books and records violations
- (3) Internal control weaknesses

e) Money laundering

f) Aiding and abetting fraud by other parties (customers, vendors)

Annex 3

RECOMMENDED CONTROLS FOR MITIGATION

1. CHOICE OF THE APPLICANT BID

Comprehensive controls

- Secondary Board (Commission for Appeals on public procurement) could reconsider individual decisions or sample of decisions made by the Commission for evaluation of bids
- Adequate training on ethics and integrity which covers individual responsibilities, if it is necessary
- Using tools (software) for in-depth data analysis,
- Regular independent audits (eg, internal audit, SAO or Audit Authority)
- In the case of suspected fraudulent behavior can establish a mechanism of whistleblowers

Specific risk of fraud	Control description	Recommended control fro mitigation
Conflict of interest in the commission for evaluation False statement of the applicant on offer Double funding	Selection of applicants of bid ▪ Publication of all calls for tenders. ▪ All offers are recorded. ▪ All offers are evaluated in accordance with the applicable criteria. ▪ All decisions on acceptance / rejection of tenders are submitted to applicants. Audit trail ▪ It is necessary to establish procedures that will ensure the retention of all documents required to ensure an adequate audit trail. Accounting, monitoring and financial reporting systems ▪ An accounting system that provides reliable and relevant information functions effectively.	▪ Evaluation Commission is composed of several members of senior management that can be changed, and whose election to participate in each panel for evaluation to a certain degree at random. ▪ **Policy on conflicts of interest** with an annual statement and registry / registry.
		▪ Cross-checking the supporting documents from independent sources of evidence. ▪ Use prior knowledge of the bidder in making good / wise decision regarding the authenticity of the statements and information provided.
		▪ Cross-checking with the competent authorities, where this is possible, and it estimates that the risk is relevant and that there is a certain probability that it will be happen.

2. IMPLEMENTING AND CHECK / CONFIRMATION OF ACTIVITIES
Comprehensive controls
▪ Request the public sector entities to have a policy on conflict of interest, with an annual statement and register ▪ Provide training to detect fraudulent behavior within the public sector entities ▪ Using tools for in-depth data analysis ▪ Establishing a mechanism of reporting in a case of the suspicion of fraudulent behavior ▪ Effective check on management ▪ Compliance with national requirements for independent audit of the project costs incurred in entities

Specific risk of fraud	Description of control	Recommended control for mitigation
Divided procurement ------------------------ Unjustified direct agreements to avoid bidding ------------------------ Lack of procedure for bidding for individual suppliers ------------------------ Extension of existing contracts to avoid re-announcement of bidding ------------------------ Adjusted specifications in favor of certain users ------------------------ Unauthorized disclosure of data supply Undeclared conflict of interest ------------------------ Bribery ------------------------	**Guidelines for users** ▪ Efective communication with consumers about their rights and obligations, in particular for national rules for participation that are prescribed for the program , special requirements in terms of products or services that are need to be submitted as part of the operation, the financing plan, the time limit for execution, requirements concerning separate accounting or relevant items accounting, information to be stored and submit / publish . ▪ The existence of clear and unambiguous national rules on participation / eligibility prescribed for the program. ▪ Existence of a strategy that will ensure that users have access to the necessary information and receive appropriate guidance. **Management checks** ▪ The existence of written procedures and comprehensive check lists for check management ▪ Check management which should be completed before confirmation ▪ All claims for compensation may be management body to administrative review, including review of applications and accompanying documentation	▪ If necessary, management body review the list of proposed contracts under the threshold of the entity, before implementation of the program -- ------ --------------- ▪ The management body review on a sample of direct agreements of users. ▪ Prior authorization from the management body of any direct agreements. -- --------------- ------ ▪ Management body reviewing a sample of contracts with large value before the invoice as evidence of the tender. -- ---------------------- ▪ The management body previously approved changes in the agreement that the original contract extends over a significant predefined threshold. ▪ -- ---------------------- ▪ The application of the management body users to have a secondary mechanism, in addition to procurement department, which will check the specifications of the bids are too short. The management body shall review the functioning of this control sample of users . -- --------------------- ▪ The application of the management body users to have a secondary mechanism, which compares a sample of a successful offer with competitive bids, seeking clues to previously having data from bids. The management body shall review the functioning of this control sample of users . ▪ The application of the management body a high degree of transparency in the award of contracts, such as releasing all the data from the agreement that are not sensitive to the public. The management body shall review the functioning of this control sample of users . ▪ Management body reviewed a sample of successful bid compared with the competition seeking clues about prior knowledge of information on bidding. ▪ -- ----------------- ---- ▪ **Conflict of interest policy,** with the annual statement and

Collusion ----------------------------- Manipulation of tenders ----------------------------------- Deficiencies in pricing ---------------------------- "Nonexistent" service ---------------------------- One contractor reported double costs ---------------------------- Replacement Product ---------------------------- Lack of products or failure to operate in accordance with the agreement grants among st st ----------------------------- False, or double inflated invoices -----------------------------	▪ Field checking which is carried out when the project is at an advanced stage of construction ▪ Stored evidence on the activities and results and findings are following ▪ Sampling should be based on proper risk assessment ▪ Existence of procedures that will ensure that the certifying authority receives all necessary information **Audit trail** ▪ The management body should have accounting records which contained detailed information on the costs incurred in each co-financed operation ▪ The technical specifications and financial plan of the operation, progress reports and monitoring, documents for bids, evaluation, selection, approval of grants and procedures for bidding and procedures for contracts and inspection reports of the co-financed products and services should be kept on appropriate management level ▪ An management body should check whether the users have a separate accounting system or a separate accounting code for all transactions ▪ It is necessary to establish procedures that will ensure the retention of all documents required to ensure an adequate audit trail. **Accounting, monitoring and financial reporting systems** ▪ Accounting system, that provides reliable and relevant information, efficiently functioning.	register -- --------------- ------ ▪ The application of the management body users to have strong control of tender procedures, such as strict respect of deadlines for submission of tenders. Management body to review the functioning of this control sample of users . ▪ The application of the management body users to review all contracts awarded by a secondary mechanism seeking clues as great closeness of the successful bids in the next lowest bid in a row, winning the later submitted bids and / or evidence that the successful bidder privately communicated with persons that participating in conducting the auction. Management body to review the functioning of this control sample of users . ▪ Management body review sample of the successful bid seeking clues as great closeness of the successful bid with the next lowest bid in a row, winning the later submitted bids and / or evidence that the successful bidder privately communicated with persons that participating in the implementation of the tender may indicate fraudulent behavior. -- ---------------- ----------- ▪ Request management body on the suppliers have established controls to detect particularly high or unusual data in bids (such as evaluators who know the market) and unusual relationships between third parties (eg. Rotation of the contract). Management body to review the functioning of this control sample of users . ▪ Request management body users to establish "standards," to compare the prices of standard products or services. Management body to review the functioning of this control sample of users . -- ---------------- ---------- ▪ Request management body users are bidding procedure which includes transparency in the procedure for opening tenders and appropriate security arrangements for unopened bids. Management body to review the functioning of this control sample of users . -- ----------------- --------- ▪ Request management body users establish controls to check the prices listed third countries compared with independent sources. Management body to review the functioning of this control sample of users . ▪ Request management body users to use the standard unit costs for regular supply. -- ------------------------- ▪ Request management body users to perform a full background check on all third parties. This may include a general inspection of web pages locationof the company, contact information and the like. Management body to review the functioning of this control sample of users . -- ------------------------- ▪ Request management body users to pre investigate working

		reports and results from contract request evidence of costs you (eg. Names of employees) and that the agreement of their allowed to require additional evidence (eg, systems for records of working time). Management body to review the functioning of this control sample of users . -- -------------------------- ▪ Request management body users to compare the purchased products / services with the specification of the contract, using relevant experts. Management body to review the functioning of this control sample of users . ▪ Management body reviewed the working report and certain purchased products / services compared with the specifications in the contract. -- -------------------------- ▪ Request management body users to seek confirmation for work or other forms of certificate verification, awarded by an independent third party after completion of the contract. Management body to review the functioning of this control sample of users . ▪ Management body checked copy of the work or other forms of certificate authentication -- -------------------------- ▪ Request management body users to check the e forsaken invoices in order to detect possible twofold issue (ie more invoices with the same amount, invoice number, etc.) or forgery. Management body to review the functioning of this control sample of users . ▪ Request management body users to compare the closing price of the products / services in the invoice with generally accepted prices for similar contracts. Management body to review the functioning of this control sample of users . ▪ Management body review copy of the results of the project in terms of cost in search of evidence that the work is not completed or that the costs incurred were necessary.

Annex 3

RECOMMENDED MITIGATE CONTROLS

2. IMPLEMENTATION AND CHECK / CONFIRMATION OF ACTIVITIES

Comprehensive controls

- In cases of suspected fraudulent behavior can establish a mechanism of whistleblowers.
- Using the tool for in-depth data analysis
- Effective management verification
- Compliance with national requirements for independent audit of the project costs that are incurred in users

Specific risk of fraud	Description of control	Recommended mitigate controls (or specific checks that must be included in the management verification)
The reported costs for inadequate skilled staff ---------- ---------------------------- False labor costs Unpaid overtime work reported as real expenditure	**User guide** • Effectively inform users of their rights and obligations, in particular national rules for eligibility prescribed for program, specific requirements in terms of product or services to be delivered as part of the activity, the financial plan, the time limit for execution, conditions about separate accounting or adequate accounting codes, information that should be kept and communicated. • Existence of clear and unambiguous national eligibility rules of eligibility prescribed for the program. • Existence of a strategy that will ensure users have access to the necessary information and receive appropriate instructions. **Check management** ▪ The existence of written procedures and comprehensive check lists for checking and management verification • All claims for compensation may to be subject on administrative review, including review of applications and accompanying documentation • Spot check which is carried out when the project is at an advanced stage of implementation • Evidence on the performed activities are held and received results are follow • Sampling must be based on proper risk assessment • Existence of procedures that will ensure that verification body gets all the necessary information	• Reviewing the final performance reports and financial statements looking for differences between planned and actual number of employees. • Request for additional evidence (eg. Confirmations of qualification), as confirmed the appropriateness of the significant reimbursements • Prior approval of significant changes in key personnel • Request bidders to check key personnel to third parties participating in the implementation of the agreement in respect of employees in the proposed supply and demand evidence that confirming the appropriateness of significant recoveries. Management body reviews the functioning of these controls on a sample of users. • Users request of third countries to give prior approval for significant changes in staff. Management body reviews the functioning of these controls on a sample of users. --- ---------- • Check evidence that the bidders submited for completion of the project activities, for example, registers and systems for recording working time. • Review of final work reports and financial reports received from users looking for differences between planned and actual activities. • Request bidders to review evidence on the implemented activities submitted by third parties, for example, registers and records of working time. Management body to review the functioning of these controls on a sample of users. • Review of final work reports and financial statements looking for differences between planned and actual activities. Management body reviews the functioning of these controls on a sample of users.

-------------------------------------- Reported incorrect salary per hour ----------- --------------------------- Costs for work incorrectly allocated between projects --------- ---------------------------- Incorrect descriptions of the activities that employees are performed ----------- --------------------------- Reported costs for employees, employees who did not exist	**Audit trail** • The management body must keep accounting records which contains all the detailed information about costs genuinely incurred by the bidder in each co-financed activities • The technical specifications and financial plan for the operation, progress reports and monitoring, documents for tender, evaluation, selection, approval of grants and tender procedures and contracting procedures, and reports for review of co-financed products and services should be kept at the appropriate management level. • Management body should check whether the users have a separate accounting system or separate accounting code for all transactions • It is necessary to establish procedures that will ensure the retention of all documents required to ensure an adequate audit trail. **Accounting, monitoring and financial reporting systems** Computer system that provides reliable and relevant information, efficiently work.	-- ---------- • Review of the final financial statements and reports for work and accompanying documentation, which looking for clues that the notified overtime (excessive working hours for employees who participated in the project implementation, a smaller number of employees than planned, but implemented all activities). • Request users to compare invoices from suppliers with the associated documents in search of clues that is reported overtime (excessive working hours for employees who participated in the project implementation, a smaller number of employees than planned). Management body reviews the functioning of these controls on a sample of users. -- ---------- • Comparison of the final financial report with evidence of their actual wage costs (for example, contracts, payed lists) and spent working time on the project activities (eg. Systems for registering working time, records of working hours). • For labor costs from third parties - management body requires the bidder to review invoices for staff costs in relation to the evidence of actual costs incurred to pay (for example, contracts, payed lists) and spent working time on the project activities (eg systems for recording working time registers). All evidence considered with appropriate skepticism. Management body reviews the functioning of these controls on a sample of users. -- ---------- • Reviewing the evidence from the supplier in order to independently verify the allocation of staff costs for project activities, such as registers, systems for recording working time data from business records. -- ---- • Check evidence from the supplier, in order to independent verification of the final project activities, for example, registers and systems for recording working time. • Reviewing the final work reports and financial statements looking for differences between planned and actual activities. • Request suppliers to check the evidence supplied by third parties to independently verify the completion of activities, for example, registers and systems for recording working time. Management body reviews the functioning of these controls on a sample of users. • Request suppliers to review the final reports and financial statements looking for differences between planned and actual activities. Management

----------- --------------------------- Staff costs reported for activities implemented outside the period of execution of works		body reviews the functioning of these controls on a sample of users. -- ---- • Reviewing the evidence of suppliers to independently verify the existence of employees, for example, contracts, social security data. • Request suppliers to examine evidence from third parties that may independently verify the existence of employees, for example contracts, details of social security. Management body reviews the functioning of these controls on a sample of users. -- ---- • Reviewing the evidence of the supplier on the basis of which may independently check whether the costs are made within the deadlines for implementation of the project, for example, original invoices, bank statements / conclusions. • Request suppliers to examine evidence from third parties that may independently verify that costs incurred within the deadlines for implementation of the project, for example, original invoices, bank statements / conclusions. Management body reviews the functioning of these controls on a sample of users.

Annex 3

RECOMMENDED CONTROLS TO MITIGATE

3. ENDORSEMENT / CONFIRMATION AND PAYMENT

Comprehensive controls

- Conflict of interest, with an annual statement and register
- Effective check on management
- In the case of suspected fraudulent behavior can establish a mechanism of whistleblowers
- Regular adequate training courses on ethics and integrity that include individual responsibilities

Specific risk of fraud	Description of control	Recommended mitigate controls
Incomplete / improper procedure for checking that the management does not provide sufficient insurance of the fraud -------------------------------- Incomplete / improper procedure for verifying that does not provide sufficient insurance of the fraud ------------------------------ Conflicts of interest in management body have inadequate / improper influence on payments approval ----------------------------------- Conflicts of interest in verification body have an inadequate / improper influence on payments approval	**Distribution of functions within the management body and bodies for endorsement** • Clearly defined and distributed functions **Check of management** • Existence of written procedures and comprehensive management checklist • Estimation of management which should be completed before verification • All requests for payments may be subject to administrative review, including a review of applications and accompanying documentation • Spot checks that are carried out when the project is at an advanced stage of implementation • Evidence of performed activities and the results are stored and monitored findings • Sampling must be based on proper risk assessment • Existence of procedures that will ensure the body for endorsement to receive all necessary information **Endorsement / validation** ▪ Body endorsement must keep proper accounting records in electronic form.	▪ Management body performed secondary extensive review of sample to verify management, ensuring is it carried out in accordance with the relevant guidelines and standards. ▪ Employees who certify expenditures are appropriately qualified and trained and have undergone a course of updating the knowledge of fraud. The management body shall review the appropriateness of such training programs. ▪ Audit body review certify expenditure carried out by a certification body ensuring that they are made in accordance with the relevant guidelines and standards. ▪ Payment process consists of several separate stages of approval, with prior approval is required to provide evidence for justifying the expenditure (eg. An independent audit opinion).

	▪ With the audit trail in the body for endorsement should enable the adjustment of declared expenditure with reports received from the management body . ▪ Endorsement body has indicated what data are needs for procedures that implement management body for verification of expenditure and has established procedures that will ensure that the same time will be received. ▪ Endorsement body is considering prepeared reports by the management body ▪ Endorsement body reviewing the results of any revisions ▪ Endorsement body ensure that the results of these reviews are completely take in account ▪ Endorsement body coordinates and executes arithmetic checking for payment requeasts.	The process of endorsement / validation consists of several separate stages of approval before providing confirmation foundedness on expenditures.

Annex 4

ANTI-FRAUD POLICY[14] TEMPLATE

[*This template suggests how the managing authority (MA), could structure its anti-fraud policy statement, and also includes a commitment from the audit authority*]

Introduction

The Managing Authority (MA) of *[insert the name of institution]* is committed to maintain high legal, ethical and moral standards, to adhere to the principles of integrity, objectivity and honesty and wishes to be seen as opposed to fraud and corruption in the way that it conducts its business. All members of staff are expected to share this commitment. The objective of this policy is to promote a culture which deters fraudulent activity and to facilitate the prevention and detection of fraud and the development of procedures which will aid in the investigation of fraud and related offences and which will ensure that such cases are dealt with timely and appropriately.

A procedure is in place for the disclosure of situations of conflict of interests.

The term fraud is commonly used to describe a wide range of misconducts including theft, corruption, embezzlement, bribery, forgery, misrepresentation, collusion, money laundering and concealment of material facts. It often involves the use of deception to make a personal gain for oneself, a connected person or a third party, or a loss for another – intention is the key element that distinguishes fraud from irregularity. Fraud does not just have a potential financial impact, but it can cause damage to the reputation of an organisation responsible for managing funds effectively and efficiently. This is of particular importance for a public organisation responsible for the management of EU funds. Corruption is the abuse of power for private gain. Conflict of interests exists where the impartial and objective exercise of the official functions of a person are compromised for reasons involving family, emotional life, political or national affinity, economic interest or any other shared interest with e.g. an applicant for or a recipient of EU funds.

Responsibilities

Within the MA, overall responsibility for managing the risk of fraud and corruption has been delegated to *[insert details of department or person]* who has the responsibility for:

  - Undertaking a regular review, with the help of a risk assessment team, of the fraud risk;
  - Establishing an effective anti-fraud policy and fraud response plan;
  - Ensuring fraud awareness of staff and training;
  - Ensuring that the MA refers promptly investigations to competent investigation bodies when they occur;

- Process owners/managers of the MA are responsible for the day-to-day management of fraud risks and action plans, as set out in the fraud risk assessment and particularly for:

[14] The anti-fraud policy statement, together with procedures for adequate fraud risk assessment and the putting in place of effective and proportionate anti-fraud measures through an action plan (whenever the net risk after controls is significant or critical), are key components of the managing authority's anti-fraud programme or strategy.

    - Ensuring that an adequate system of internal control exists within their area of responsibility;
    - Preventing and detecting fraud;
    - Ensuring due diligence and implementing precautionary actions in case of suspicion of fraud
    - Taking corrective measures, including any administrative penalties, as relevant.
- The Certifying Authorities have a system which records and stores reliable information on each operation; they receive adequate information from the MA on the procedures and verifications carried out in relation to expenditure.
- The Audit Authority has a responsibility to act in accordance within professional standards[15] in assessing the risk of fraud and the adequacy of the control framework in place.

Reporting Fraud

The MA has procedures in place for reporting fraud, both internally and to the European Anti-Fraud Office […….insert details of internal reporting lines and those reporting to the European Anti-Fraud Office….].

All reports will be dealt with in the strictest of confidence and in accordance with […insert details of relevant Data Protection/Disclosure Act…]. Staff reporting irregularities or suspected frauds are protected from reprisals.

Anti-fraud measures

The MA has put in place proportionate anti-fraud measures based on a thorough fraud risk assessment . In particular, it uses IT tools to detect risky operations (if it is developed) and ensures that staff is aware of fraud risks and receives anti-fraud training. The MA carries out a vigorous and prompt review into all cases of suspected and actual fraud which have occurred with a view to improve the internal management and control system where necessary. […insert details of review procedures…].

Conclusion

Fraud can manifest itself in many different ways. The MA has a zero tolerance policy to fraud and corruption, and has in place a robust control system that is designed to prevent and detect, as far as is practicable, acts of fraud and correct their impact, should they occur.

[Delete or retain, as relevant:] This policy and all relevant procedures and strategies are supported by the […insert title of oversight body who will approve the Fraud Policy e.g. a Board..] who will proactively review and update them on a continual basis.

[15] International Standards for the Professional Practice of Internal Auditing, International Standards on Auditing

Annex 5

Compliance check of the managerial body
Assessing the risk of fraud and effective and proportionate measures against fraud for the period from ----- to -----

		Prepared	Reviewed
C.0.	List of problems		
C1.1.	Assessment process		
C 1.2.	Gross risk		
C.1.3.	Existing controls and net risk		
C.1.4.	Action plan and target risk		

Annex 5

C.0 - List of problems

Reference number of the test/re-examined	Identified problems	Respond of the managerial authority	Resolved

Annex 5

C1.1	Assessment process	Y / N n / a	Remarks
	Review the Risk Assessment Implementation Procedure Fraud and consider the following questions:		
1.	Was the assessment team composed of persons with adequate knowledge and experience in the areas of risk fraud and related responses, making and operating effectiveness of control, risk assessment?		
2.	Has enough time and resources been spent on the procedure to could be considered meaningful and credible process?		
3.	Are there any evidence that they are taking the risk assessment procedure, consider sources of information such as audit reports, fraud reports and self-assessment of controls?		
4.	Is the self-assessment procedure clear and permissible a clear review of the conclusions reached?		
5.	There is evidence that senior management is sufficiently large supervised the procedure and / or participated in the proceedings and that approved the net exposure level?		
C1.2.	**Gross risks**	**Y / N n / a**	**Remarks**
	Sample Selection: Select an example of benchmark risk from the evaluation tool risk of fraud. The pattern should be covered following: ▪ all the procedures (1) selection of the applicant, 2) Implementation of the program, 3) certification and payment, and 4) Direct procurement of the management body (if applicable)) ▪ risks from all categories of rating gross risk (bearable,significant and critical) For each of these risks, perform the following tests:		
First	Review the impact of risk score (GROSS) in relation to scale rating to "Guidelines on the assessment of the risks of fraud ". Is the grade consistent with the following: ▪ explanations that submitted the assessment team, ▪ supporting evidence provided by the assessment team, ▪ your knowledge of the environment GROSS risk.		
Second	Review the likelihood of risk (GROSS) in relation on the scale score in the "Guidelines on the assessment of the risks of fraud ". Is the grade consistent with the following: ▪ explanations that submitted the assessment team, ▪ supporting evidence provided by the assessment team, ▪ your knowledge of the environment GROSS risk.		
Third	Is the total GROWTH risk calculated correctly and is it correct rated (tolerable, substantial, critical)?		
C.1.3.	**Existing controls and net risk**	**Y / N n / a**	**Remarks**
	Sample Selection: Select an example of benchmark risk from the evaluation tool risk of fraud. The pattern should be covered following: ▪ all the procedures (1) selection of the applicant, 2) Implementation of the program, 3) certification and payment, and 4) Direct procurement of the management body (if applicable))		

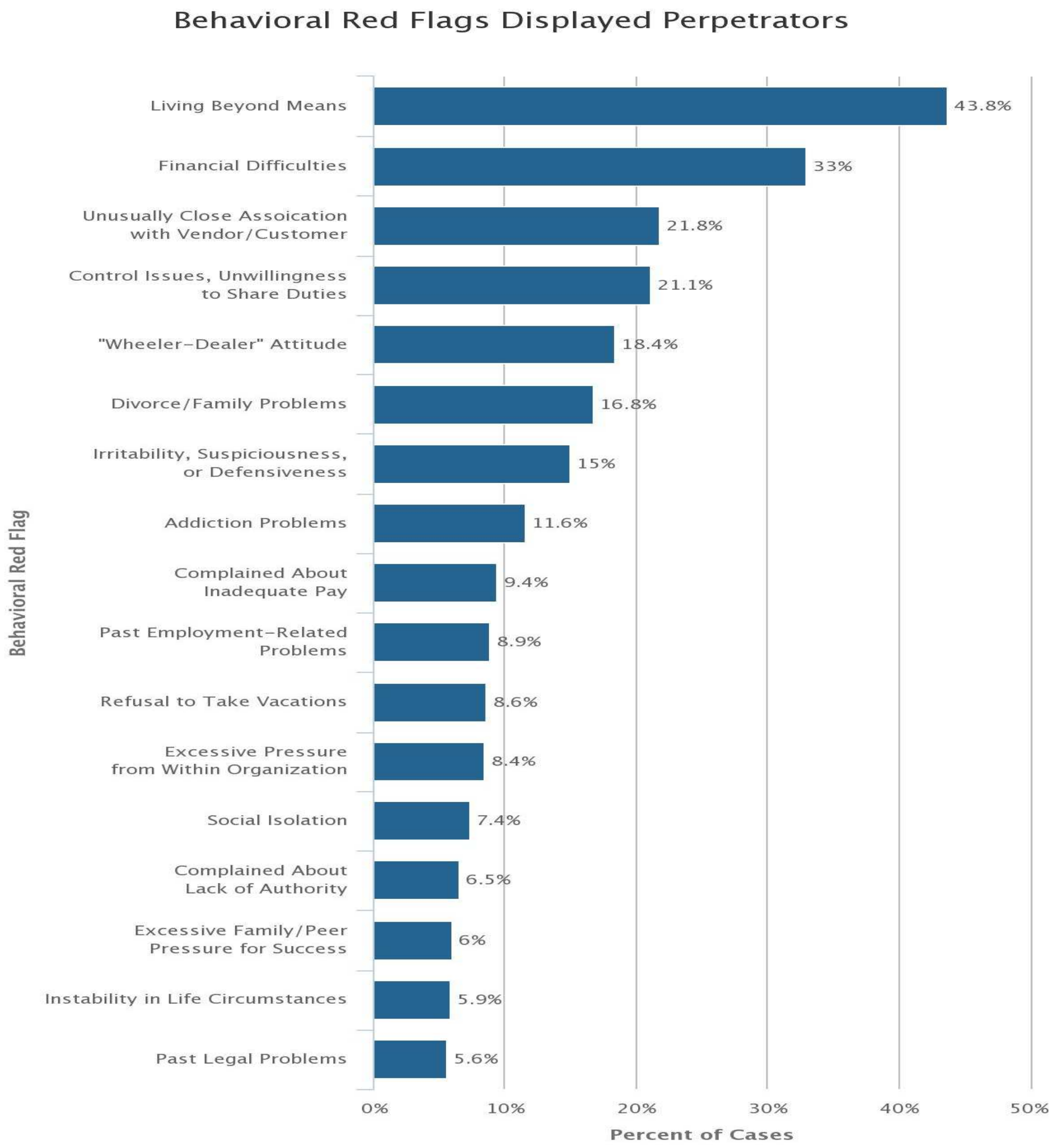
	▪ risks in the context of a substantial score and critical GROSS risk. For each of these risks, perform the following tests:		
1.	Review your existing control data recorded the evaluation team. For each, confirm the following:		
a.	Are there any of that control?		
b.	Do you agree with the response team to assess in this connection is is the application of these controls recorded? Are there any paper evidence of it?		
c.	Do you agree with the assessment team's response to that Are the controls regularly questioned? There is paper evidence about that?		
2.	Review the efficiency check of the combined controls on the EFFECT of gross risk. Is the grade consistent with the following: ▪ Your knowledge of the effectiveness of control structures in with regard to the mitigation of specific risk, ▪ Supporting evidence confirming that control they work effectively (based on tests that conducted by the governing body, the audit body, the intermediary body or other audit body).		
3.	Review the efficiency check of the combined controls on the LIKELIHOOD of gross risk. Is the grade consistent with the following: ▪ Your knowledge of the effectiveness of control structures in with regard to the mitigation of specific risk, ▪ Supporting evidence confirming that control they work effectively (based on tests that conducted by the governing body, the audit body, the intermediary body or other audit body).		
4.	Is the total NET risk calculated correctly and is it correct rated (tolerable, substantial, critical)?		
C.1.4.	**Action plan and target risk**		
	Sample Selection: Select an example of benchmark risk from the evaluation tool risk of fraud. The pattern should be covered following: ▪ all the procedures (1) selection of the applicant, 2) Implementation of the program, 3) certification and payment, and 4) Direct procurement of the management body (if applicable)) ▪ risks in the context of a substantial score and critical NET risk. For each of these risks, perform the following tests:		
1.	Review the performance review of planned new controls On the EFFECT of net risk. Is the grade consistent with the following: ▪ your knowledge of the effectiveness of control structures in with regard to the mitigation of specific risk.		
2.	Review the performance review of planned new controls on LIKELIHOOD of net risk. Is the grade consistent with following: ▪ your knowledge of the effectiveness of control structures in with regard to the mitigation of specific risk.		
3.	Is the total TARGET risk calculated correctly and is it correct rated (tolerable, substantial, critical)?		
4.	It seems that additional optimum controls are planned and well thought out?		

Annex 6

Behavioral Red Flags Displayed Perpetrators

Usually professional fraudsters exhibit certain traits of behavior and characteristics in the performance of their schemes. In 92% of cases analyzed, the deceiver showed at least one of these red flags of behavior, and in 64% of cases were observed more red flags before the detection of fraud. Understanding that these traces of behavior are indicators of fraudulent conduct, which may improve our ability to detect occupational fraud at an early stage and minimize it`s costs.

The table below shows the percentage of cases in which are placed the various red flags in behavior.[16]



© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved

[16] See link http://www.acfe.com/rttn-red-flags.aspx as red flags in behavior differ based on the following factors: the position of the offender, type of fraud and sex offender.

Annex 7

CONTRACT AND PUBLIC PROCUREMENT FRAUD[17]

Common and recurrent fraud schemes and the relevant fraud indicators (red flags)

This annex lists sixteen common and recurrent fraud schemes with a description of the scheme and the relevant fraud indicators in the area of contracts and public procurement.

This is a non-exhaustive list of generally recognised schemes.

This annex uses much of the structure and contents which ACFE[18] applies in its instruction for professionals in the field of fraud prevention and detection.

1. Corruption – bribes and kickbacks

Scheme description:

Bribes and kickbacks refer to the giving or receiving of a "thing of value" to influence an official act or a business decision.

Corrupt payments

The "thing of value" need not be money, and often is not (the ambiguity remains and the perpetrator can more easily invent excuses if needed)**.** Any tangible benefit given or received with the intent to corruptly influence the recipient can be a bribe. Specific "things of value" that have been given and received as bribes include e.g.: gifts whose value exceeds thresholds set by organisations/companies, "loans" whether or not repaid, use of credit cards, overpaying for purchases (e.g. paying € 500,000 for an apartment worth € 200,000), free use of apartment, or discounted rent, free use of a leased car, cash payments, payment by check or bank transfer of false "fees or commissions", often an agreed percentage of the contract obtained, and paid through a middleman or a *shell company*[19] set up by the recipient and hidden ownership interest in the corrupt contractor or seller). The things of value are often given in the order of this listing. This is because the parties may be unsure of the other's intentions at the outset and the bribe payer may not be able to afford more substantial payments until a contract is awarded.

After the contract award, most bribes are paid in the form of kickbacks, meaning that the contractor will pay or "kickback" an agreed percentage of each invoice payment it receives. Whatever manner the bribes are paid, prices are usually inflated or the quality of goods and services reduced, to cover the cost of the payments.

Corrupt payments facilitate many other types of fraud, such as false invoicing, phantom expenditure or failure to meet contract specifications.

Corrupt influence

Corrupt influence in the contract and procurement area is often reflected as: improper selection such as unjustified single source acquisition (there might be multiple awards under the threshold for public procurement), unjustified high prices, excessive quantity of purchases, acceptance of low quality and delayed or no delivery.[20]

[17] Information Note on Fraud Indicators for ERDF, ESF and CF http://ec.europa.eu/regional_policy/sources/docoffic/cocof/2009/cocof_09_0003_00_en.pdf

[18] Association of Certified Fraud Examiners, www.acfe.com. More specifically, the structure and contents draw on the "Contract and Procurement Fraud" training for Fraud Examiners.

[19] A shell company is a company that does exist but does not actually do any business or have any assets.

[20] This is often summarised as the "SPQQD" factors: improper Selection, high Price, excessive Quantity, low Quality, delayed or no Delivery.

Fraud indicators:

The most common indicator of bribes and kickbacks is unexplained favourable treatment of a contractor by a contracting employee over a period of time.

Other red flags:

- close socialisation between a contracting employee and service or product provider;
- unexplained or sudden increase in wealth by the contracting employee;
- contracting employee has an undisclosed outside business;
- contractor has a reputation in the industry for paying kickbacks;
- undocumented or frequent changes to contracts increasing the value of the contract;
- contacting employee declines promotion to a non-procurement position;
- contracting employee fails to file or complete conflict of interest declaration.

2. Undisclosed conflict of interest

Scheme description:

A situation of conflict of interest can occur if an employee of the contracting organisation has an undisclosed financial interest in a contract or contractor.

A potential conflict of interest might be immune from legal action if it is fully disclosed and approved by the employer in a timely manner. An employee might e.g. secretly own a supplier or a contractor, set up a shell company through which he or she purchases supplies at an inflated price or have an undisclosed interest in property sales or leases.

Fraud indicators:

- unexplained or unusual favouritism of a particular contractor or seller;
- continued acceptance of high priced, low quality work etc;
- contracting employee fails to file or complete conflict of interest declaration;
- contacting employee declines promotion to a non-procurement position;
- contracting employee appears to conduct side business.

3. Collusive bidding

Scheme description:

Contractors in a particular geographic area or region or industry can conspire to defeat competition and raise prices through various collusive bidding schemes.

Complementary bidding

Complementary bids, also known as "shadow" bids, are intended only to give the appearance of genuine bidding and not to secure the buyer's acceptance. Cooperating bidders agree to submit higher priced or deliberately non-responsive bids to allow the selection of a favoured contractor at an inflated price. The winner shares a percentage of its profits with the losing bidders, hires them as subcontractors, or allows them to win other high priced contracts. Complementary bids may also be submitted from shell companies or from affiliated firms.

Bid suppression

For bid rigging schemes to succeed the number of bidders must be limited and all must agree to the conspiracy. If a new (a so-called "diver") or uncooperative bidder enters the competition, the price inflation will become apparent. To prevent this, the conspirators may pay-off outside companies not to bid or use more forceful means to discourage their participation. The conspirators can also coerce suppliers and subcontractors not to deal with non-cooperating companies to protect their monopoly.

Bid rotation

The conspirators submit complementary bids or refrain from bidding in order to allow each bidder to be the low bidder on a rotating basis. The rotation can be based on geographic area – one road contractor gets all work in one region, another company in the next – or by type of job, or by time, etc.

Market division

The cooperating companies may divide markets or product lines and agree not to compete in each other's area, or to do so through collusive measures, such as submitting only complementary bids. Sometimes employees may be involved in collusive bidding schemes – sometimes with a financial interest in the "competing" businesses – and receive a share of the inflated prices.

Fraud indicators:

- winning bid is too high compared to cost estimates, published price lists, similar works or services or industry averages and fair market prices;
- persistent high prices by all bidders;
- bid prices drop when new bidder enters the competition;
- rotation of winning bidders by region, job, type of work;
- losing bidders hired as subcontractors;
- unusual bid patterns (e.g. the bids are exact percentage apart, winning bid just under threshold of acceptable prices, exactly at budget price, too high, too close, too far apart, round numbers, incomplete, etc);
- apparent connections between bidders, e.g. common addresses, personnel, phone numbers etc;
- contractor includes subcontractors in its bid which are competing for the main contract;
- qualified contractors fail to bid and become subcontractors or low bidder withdraws and becomes a subcontractor;
- certain companies always bid against each other, others never do;
- losing bidders cannot be located in the Internet, business directories, have no address
- etc (in other words they are fictive);
- correspondence or other indications that contractors exchange pricing information, divide territories, or otherwise enter informal agreements;
- collusive bidding has been found in the following sectors and is also relevant for structural funds: asphalt paving, building construction, dredging, electrical equipment, roofing, waste disposal.

4. Unbalanced bidding

Scheme description:

In this fraud scheme contracting personnel provide a favoured bidder with useful inside information which is not available to other bidders, for example, that one or several line items in a request for bid will not be used in the contract (some line items may also be vague or ambitious on purpose and the favoured bidder is instructed how to respond).

This information allows the favoured firm to submit a lower price than the other bidders, by quoting a very low price on the line item which will not be included in the final contract.

Unbalanced bidding is one of the more effective bid rigging schemes as the manipulation is not as obvious as in other popular schemes, such as unjustified single source acquisitions.

Fraud indicators:

- particular line item bids appear to be unreasonably low;
- changes are issued soon after contract awards to delete or modify line item requirements;
- line items for bids are different than the actual contract;
- bidder close to procurement personnel or participated in drafting specifications.

5. Rigged specifications

Scheme description:

Requests for bids or proposals might contain specifications which are tailored to meet the qualifications of a particular bidder, or which only one bidder can meet. This is particularly common in IT and other technical contracts.

Specifications which are too narrow can be used to exclude other qualified bidders, or to justify single source acquisitions and avoid competition altogether. A pattern of rigged specifications which favour a particular contractor suggests corruption.

Fraud indicators:

- only one or a few bidders respond to request for bids;
- similarity between specifications and winning contractor’s product or services;
- complaints from other bidders;
- specifications are significantly narrower or broader than similar previous requests for bids;
- unusual or unreasonable specifications;
- high number of competitive awards to one supplier;
- socialisation or personal contacts between contracting personnel and bidders during the bidding process;
- the buyer defines an item using brand name rather than generic description.

6. Leaking bid data

Scheme description:

Contracting, project design or bid evaluation personnel can leak confidential information to help a favoured bidder formulate a technical or financial proposal, such as estimated budgets, preferred solutions, or the details of competing bids.

Fraud indicators:

- poor controls on bidding procedures, e.g. failure to enforce deadlines;
- winning bid just under the next lowest bid;
- some bids opened early;
- acceptance of late bids;
- late bidder is the winning low bidder;

- all bids are rejected and contract is re-bid;
- winning bidder communicates privately with contracting personnel by e-mail or otherwise during bidding period.

7. Manipulation of bids

Scheme description:

In a poorly controlled bidding process contracting personnel can manipulate bids after receipt to ensure that a favoured contractor is selected (changing bids, "losing" bids, voiding bids for alleged errors in specifications, etc)

Fraud indicators:

- complaints from bidders;
- poor controls and inadequate bidding procedures;
- indications of changes to bids after reception;
- bids voided for errors;
- a qualified bidder disqualified for questionable reasons;
- job not re-bid even though fewer than the minimum number of bids were received.

8. Unjustified single source awards

Scheme description:

This scheme often results from corruption, in particular if the pattern is repeated and questionable.

Such awards can be made by splitting purchases to avoid competitive bidding thresholds, falsifying single source acquisition justification, drafting very narrow specifications, extending previously awarded contracts rather than re-bidding.

Fraud indicators:

- single source awards above or just below competitive bidding thresholds;
- previously competitive procurements become non-competitive;
- split purchases to avoid competitive bidding threshold;
- request for bid mailed only to one service provider.

9. Split purchases

Scheme description:

Contracting personnel may split a purchase into two or more purchase orders or contracts in order to avoid competition or higher-level management review. For example, if the threshold is € 250,000, a single procurement of goods and services for € 275,000 can be split into two contracts – one for goods for € 150,000 and the other for € 125,000 – to avoid bidding.

Split purchases (often called "salami slicing") can indicate corruption or other schemes by a purchasing employer.

Fraud indicators:

- two or more consecutive, related procurements from the same contractor just under
- competitive bidding or upper level review thresholds;

- unjustified separation of purchases, e.g. separate contracts for labour and materials, each of which is below bidding thresholds;
- sequential purchases just under the thresholds.

10. Co-mingling of contracts

Scheme description:

A contractor with multiple similar work orders might charge the same personnel costs, fees or expenses to several of the orders, resulting in over-invoicing

Fraud indicators:

- similar invoices presented under different jobs or contracts;
- the contractor invoices for more than one job for the same time period.

11. Cost mischarging

Scheme description:

A contractor can commit fraud by intentionally charging costs which are not allowable or reasonable, or which can not be allocated, directly or indirectly, to a contract. Labour costs are more susceptible to mischarging than material costs because employee labour can in theory be charged to any contract.

Labour costs can be manipulated by creating fictitious time sheets, altering time sheets or supporting documentation or simply invoicing for inflated labour costs without supporting documentation.

Fraud indicators:

- excessive or unusual labour charges;
- labour charges inconsistent with contract progress;
- apparent changes to time sheets;
- time sheets cannot be found;
- the same material costs charged to more than one contract;
- charging indirect costs as direct costs.

12. Defective pricing

Scheme description:

Defective pricing occurs in contracts if contractors fail to disclose current, complete and accurate cost or pricing data in their price proposals resulting in an increased contract price.

Fraud indicators:

- contractor refuses, delays or is unable to provide supporting documents for costs;
- contractor provides inadequate or incomplete documentation;
- out-of-date pricing information;
- apparent high prices compared to similar contracts, price lists or industry averages;

13. Failure to meet contract specifications

Scheme description:

Contractors which fail to meet contract specifications and then knowingly misrepresent that they have met them commit fraud.

Examples of such schemes include the use of sub-standard building materials, inferior quality parts, failure to lay the required foundation in road projects etc. The motive, of course, is to increase profits by cutting costs or to avoid penalties for failing to meet deadlines etc. Many such schemes are difficult to detect without close inspections or tests by independent subject matter experts. The fraudsters may seek to bribe the inspectors though.

Fraud indicators:

- discrepancy between test and inspection results and contract claims and specifications;
- absence of test of inspection document or certificates;
- low quality, poor performance and high number of complaints;
- indications from the contractor's expense records that the contractor did not e.g. purchase materials necessary for the works, does not own or did not lease equipment necessary for the work or did have the necessary labour on the site (NB: this type of cross-checking can be valuable).

14. False, inflated or duplicate invoices

Scheme description:

A contractor might knowingly submit false, inflated or duplicate invoices, either acting alone or in collusion with contracting personnel as the result of corruption.

Fraud indicators:

- invoiced goods or services cannot be located in inventory or accounted for;
- no acknowledgment of receipt for invoiced goods or services;
- questionable or no purchase order for invoiced goods or services;
- contractor's records do not reflect that the work was done or that the necessary costs were incurred;
- invoice prices, amounts, item descriptions or terms exceed or do not match contract items, purchase order, receiving records, inventory or usage records;
- multiple invoices with the same amount, invoice number, date etc;
- sub-contracts in cascade;
- cash payments;
- payments to off-shore companies.

15. Phantom service providers

Scheme description:

a) An employee can authorise payments to a fictitious seller in order to embezzle funds. The scheme is most common where there is a lack of segregation of duties between requisition, receipt and payment.

b) Contractors can set up phantom companies to submit complementary bids in collusive bidding schemes, to inflate costs or simply to generate fictitious invoices.

Experience has shown that fraudsters tend to use names of companies which are similar to the names of real companies.

Fraud indicators:

- service provider can not be found in any directories, the Internet, Google and other search engines etc;
- service providers address can not be found;
- the service provider lists incorrect street address or phone number;
- off-shore company used.

16. Product substitution

Scheme description:

Product substitution refers to the substitution, without the purchaser's knowledge, of inferior quality items for those which are specified in the contract. At worst, product substitution can be life-threatening, e.g. deficiencies in infrastructure or buildings.

Substitution is particularly attractive in contracts calling for expensive high grade materials that can be replaced by similar appearing, much less expensive, products. The substitution often involves component parts which are not easily detected. Specially created samples can also be presented for inspection in order to deceive.

Fraud indicators:

- unusual or generic packaging: packaging, colours or design different than the norm;
- discrepancy between expected appearance and actual appearance;
- product identification numbers differ from published or catalogue numbers or numbering system;
- above average number of test or operation failures, early replacements, or high maintenance or repair costs;
- compliance certificates signed by unqualified or non-certified person;
- significant difference between estimated and actual costs for materials;
- contactor is behind schedule but quickly catches up;
- unusual or obliterated serial numbers; serial numbers are not consistent with legitimate manufacturer's numbering system;
- invoice or inventory item numbers or descriptions do not match purchase order terms.

Annex 8

LABOUR CHARGES AND CONSULTANCY SERVICES FRAUD

Common and recurrent fraud schemes and the relevant fraud indicators (red flags)

This annex lists common and recurrent fraud schemes with a description of the scheme and the relevant fraud indicators in the area of consultancy services.

The most important control in the labour accounting system is the individual employee and the employee's acceptance of the responsibility to accurately record time worked.

This is a non-exhaustive list of generally recognised schemes:

1. Incurred labour cost

Scheme description:

Without any external independent or physical verification, labour is very vulnerable to manipulation. A promoter might knowingly claim false labour, direct and indirect. The critical issue is whether the employee's time is properly charged to the project actually worked on. (No third party documentation may exist such as invoices, purchase orders, etc., to support labour costs).

Fraud indicators:

- distinctive charging patterns;
- sudden, significant shifts in charging;
- decrease in charges to projects/contracts in overrun or near ceilings;
- a disproportionate percentage of employees charging indirect;
- large number of employees reclassified from direct to indirect or vice versa;
- same employees constantly reclassified from direct to indirect or vice versa;
- weak internal controls over labour charging, such as employee time cards signed in advance, employee time cards filled in by the supervisor, time cards filled in with pencil or time cards filled in at the end of the pay period;
- actual hours and euros consistently at or near budgeted amounts;
- use of adjusting journal entries to shift costs between contracts, R&D, commercial work;
- significant increases or decreases in charging to sensitive accounts;
- employee's time charged differently than associated travel costs.

2. Uncompensated overtime

Scheme description:

A promoter might knowingly claim false overtime where no informal credit for the extra hours, such as additional time off, is usually given. The critical issue is whether the employee's time is properly charged to the project actually worked on. No third party documentation exists.

Fraud indicators:

- professional staff required to work a significant amount of unpaid overtime on a variety of projects-both direct and indirect;
- salaried employees only charging the regular hours worked during any day for an extended period;

- a pattern of management directed unpaid overtime with employee bonus based on the extra hours worked;
- overrun contracts/projects worked on only during unpaid hours.

3. Consulting/professional service

Scheme description (based on a real case):

The services were properly supported with detailed consulting agreements, invoices and reports. The subjects covered were germane to the contractor's operations and provided appropriate recommendations to improve the efficiency of certain operations. The contractor implemented the majority of the recommendations. The applicable agreements contained the necessary level of detail and the fees were considered reasonable.

However, for some companies contracted, their services were not previously used. The agreements were not specific in what services the companies were to provide; however, they did detail who would perform the services and the hourly rate involved. The individuals' resumes were not available. The fees were higher for these new companies.

The company representative could not explain the higher fees or the specifics of what services were to be provided. Moreover, invoices from these companies for services rendered in addition were vague in describing services and only referred to the agreement. The expense was a lump sum with no breakdown of hours spent, hourly rate, travel expenses or other expenses. No trip reports or other summary reports were available. No additional information on these companies was available; the promoter was unable to provide anything other than verbal assurances of the services provided.

Finally, the invoices showed a post office box as a mailing address and no listing of these companies in the telephone directory.

Fraud indicators:

- no formal signed agreements or contracts; however, large sums paid for "services rendered" based on invoices with few specifics;
- formal agreements or contracts exist but are vague as to services to be rendered, and no other documented support, such as detailed invoices, trip reports or studies, exists to justify the expenses;
- services paid for were used to improperly obtain, distribute or use information or data protected by law or regulation;
- services paid for were intended to improperly influence the content of a solicitation, the evaluation of a proposal or quotation, the selection of sources for contract award or the negotiation of a contract, modification or claim. It does not matter whether the award is by the prime contractor or any tier subcontractor;
- services paid for were obtained or performed in some way that violated a statute or regulation prohibiting improper business practices or conflict of interest;

4. Labour categories

Scheme description (based on a real case):

A contractor's proposal for a renewal of time and material (T&M) contract, which had been awarded on a yearly basis for the last two years, indicated that the incurred hourly rates were significantly lower than the proposed rates, except for the administrative category. The original proposal had a full work force on board when the contract was originally bid. After being awarded the contract, the contractor hired/used employees at lower salaries than proposed. The qualifications of some of the newly hired employees were below the requirements per the request for proposal. The contractor had placed many of the newly hired employees in labour categories, for which they did not qualify.

Fraud indicators

- significant differences between proposed and actual unit costs or quantities with no corresponding changes in work scope or job requirements;
- task-by-task invoicing consistently at the ceiling level established in the contract. An exception would be if the contract/work order specifies how many hours to bill;
- specific individuals proposed as "key employees" not working on the contract;
- proposed labour not based on existing work force. Massive new hires needed. New hire labour rates significantly lower than proposed;
- employees' skills do not match the skill requirements as specified for their labour category or the contract requirements;
- employees typically charged indirect by the company being charged direct to the contract;
- partners', officers', supervisors' and other employees' time being charged in noncompliance with the contract terms or with the company's established accounting policies and procedures.

USED LITERATURE

1. Information Note on Fraud Indicators for ERDF, ESF and CF http://ec.europa.eu/regional_policy/sources/docoffic/cocof/2009/cocof_09_0003_00_en.pdf

2. Guidance Note On Fraud Risk Assessment And Effective And Proportionate Anti-Fraud Measures

   http://ec.europa.eu/regional_policy/sources/docgener/informat/2014/guidance_fraud_risk_assessment.pdf

3. Anti-Fraud Policy Template - https://ec.europa.eu/sfc/sites/sfc2014/files/sfc-files/guidance_fraud_risk_assessment_annex3.pdf

4. Managing the Business Risk of Fraud: A Practical Guide - http://www.theiia.org/media/files/fraud-white-paper/fraud%20paper.pdf

5. Addressing The Threat Of Fraud And Corruption In Public Procurement Review Of State Of The Art Approaches Compendium- Center For The Study Of Democracy - file:///D:/Users/Downloads/OLAF%20conference%20compendium%20EN%20(1).pdf