



Internal guidance on the methodology for fraud risk management and establishment of an anti-fraud strategy

IG Reference No: IG-009-01

Supersedes Version: EASO/EDD/2020/078

Author/Reviewer	<i>Signature on file</i>		
Approver	<i>Signature on file</i>		
Authoriser	<i>Signature on file</i>		
Status	EFFECTIVE	Approval Workflow No	<i>On file</i>
Effective Date	25-SEP-23	Review Date	24-SEP-26





Contents

Contents	2
1. Purpose and scope	3
2. Acronyms and abbreviations.....	3
3. References.....	4
4. Legal bases.....	5
5. Fraud and the motives behind it	6
5.1. Fraud.....	6
5.2. The fraud triangle - opportunity, incentive, and rationalisation.....	7
5.3. Reporting on and dealing with suspected fraud	8
6. Fraud risk management process	9
6.1. Overview.....	9
6.2. Fraud risk management objectives and priority measures.....	11
6.3. Fraud risk assessment	15
6.3.1. Scope and frequency	15
6.3.2. Identifying fraud risks.....	16
6.3.3. Assessing the likelihood and impact	17
6.3.4. Monitoring of fraud risks.....	18
6.4. Anti-fraud strategy	18
6.4.1. Scope of the anti-fraud strategy.....	18
6.4.2. Preparing the action plan to implement the anti-fraud strategy.....	19
6.4.3. Establishing related indicators and targets	19
6.4.4. Assessing and updating the anti-fraud strategy and/or the related action plan	20
6.4.5. Disclosing and communicating the anti-fraud strategy	20
7. Summary of changes	21
Annex 1: Examples of fraud indicators (or red flags)	22
Annex 2: Examples of fraud activities	26
Annex 3: Model questionnaire for the fraud risk assessment	28
Annex 4: Outline content headings of an anti-fraud strategy	40
Annex 5: Fraud risk register action plan headings	41



1. Purpose and scope

This internal guidance establishes a comprehensive methodology for fraud risk management in the EUAA and outlines the main steps for the Executive Director to propose an Agency anti-fraud strategy for adoption by the Management Board.

Fraud would impact not only the Agency’s budget, both in terms of revenue and expenditure, but would also reduce the effectiveness of the Agency’s actions, negatively impact its reputation, and undermine public trust in its initiatives. Thus, in the implementation of its budget, Article 30 of the Agency’s Financial Regulation requires it to have in place sound financial management and effective and efficient internal control that includes an appropriate risk management and control strategy to prevent, detect, and correct fraud, as well as to follow up on fraud and other irregularities.

The Agency has zero tolerance to fraud. However, it recognises that it is impossible to eliminate all risk of fraud. The purpose of this Internal Guidance is to describe the approach to managing fraud risk across all of the Agency’s business operations (not just accounting and finance) and for establishing an anti-fraud strategy.

Due to its significance and complexity, fraud risk management necessitates a separate, comprehensive approach that is performed in addition to, but in close conjunction with, the annual risk management exercise¹. The resulting output of the fraud risk management exercise is ultimately the development and implementation of an anti-fraud strategy.

The aim for adopting such an approach to fraud risk management is to deter fraud by eliminating factors that may lead to the occurrence of fraud. The Agency envisages to achieve this by:

- establishing a clear and rigorous fraud governance process and an adequate management culture that sets the tone at the top;
- creating a transparent and sound anti-fraud culture;
- performing a thorough fraud risk assessment;
- designing, implementing, and maintaining preventive and detective fraud control processes;
- responding quickly to claims of fraud, including where appropriate taking action against those involved in wrongdoing.

2. Acronyms and abbreviations

AccO	Accounting officer
AFS	Anti-fraud strategy
BSSU	Business Support and Security Unit
C1	Operational Support Centre
C2	Training and Professional Development Centre
C3	Asylum Knowledge Centre

¹ Decision of the Executive Director No 117 of 15 December 2020 on the revised risk management manual.



CAAR	Consolidated annual activity report
COSO	Committee of Sponsoring Organisations of the Treadway Commission
DPO	Data protection officer
EUAA	European Union Agency for Asylum
ED	Executive Director
EPPO	European Public Prosecutor's Office
EU	European Union
ECA	European Court of Auditors
FINU	Finance Unit
HRU	Human Resources Unit
IAS	Internal Audit Service of the Commission
ICC	Internal control coordinator
ICCU	Internal Control and Compliance Unit
ICTU	Information and Communication Technology Unit
LISO	Local information security officer
LSU	Legal Services Unit
PFMU	Procurement and Facility Management Unit
MB	Management Board
OLAF	European Anti-Fraud Office
SC	Staff Committee
SM	Senior management

3. References

This Internal Guidance refers to a list of documents and is compiled using various information sources to ensure that it adheres to the Commission's minimum standards of internal control for its own departments, as well as international best practices. The Agency's controlled governance-related documents listed below are available in ERDMS in the [EASO Legal Framework](#) library and the [EUAA Governance Framework](#) library.

- Commission Decision No 1999/352/EC, ECSC, Euratom establishing the European Anti- Fraud Office (OLAF), (OJ L 136, 31.5.1999, p. 20), as amended by Commission Decision 2013/478/EU (OJ L257, 28.9.2013, p.19), Commission Decision (EU) 2015/512 (OJ L81, 26.3.2015, p.4) and Commission Decision 2015/2418 (OJ L 333, 19.12.2015, p.148) (hereinafter 'OLAF Regulation');
- Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), (OJ L283, 31.10.2017, p.1) (hereinafter 'EPPO Regulation');
- Management Board Decision No 42 of 21 December 2018 on the Internal Control Framework of EASO;



- Management Board Decision No 54 of 14 August 2019 on the EASO Financial Regulation, as amended by Management Board Decision No 74 of 28 July 2021;
- Management Board Decision No 57 of 20 September 2019 establishing the EASO's Guidelines on Whistleblowing (hereinafter 'whistleblowing guidelines');
- Management Board Decision No 69 of 25 September 2020 on the application of the European Commission general implementing provisions on the conduct of administrative inquiries and disciplinary proceedings to EASO;
- Decision of the Executive Director No 78 of 8 April 2020 on the Manual for Fraud Risk Management (EASO/EDD/2020/078; as revised);
- COSO Internal Control—Integrated Framework and Appendices, 2013;
- COSO Enterprise Risk Management Framework, 2017;
- COSO Fraud Risk Management Guide, 2016;
- European Commission Anti-Fraud Strategy: enhanced action to protect the EU budget (COM(2019) 196 final, 29.4.2019) (hereinafter '[European Commission AFS](#)');
- European Commission Methodology and guidance for services' anti-fraud strategies, 2021 (Ref. Ares(2021)4589215, 15.7.2021) (hereinafter 'Commission AFS methodology and guidance');
- OLAF Methodology and guidance for anti-fraud strategies for EU decentralised agencies, 2013 (Ref. Ares(2013)3560341, 25.11.2013).

4. Legal bases

The legal bases for fraud risk management and an anti-fraud strategy lie in the Agency's Financial Regulation, namely the following.

- **Article 30:** The Agency's budget should be implemented in compliance with effective and efficient internal control. For the purposes of the implementation of the budget of the Agency, internal control shall be applied at all levels of management and shall be designed to provide reasonable assurance of achieving among other objectives, the prevention, detection, correction and follow-up of fraud and irregularities. Efficient internal control should be based on the implementation of an appropriate risk management and control strategy at recipient level. Efficient internal control shall be based on the implementation of an appropriate risk management and control strategy coordinated among appropriate actors involved in the control chain;
- **Article 32:** The single programming document should contain a strategy for organisational management and internal control systems including the Management Board's (MB) anti-fraud strategy as last updated and an indication of the measures to prevent recurrence of cases of conflict of interest, irregularities and fraud;
- **Article 48:** The consolidated annual activity report should contain information on organisational management and on the efficiency and effectiveness of the internal control systems including the implementation of the anti-fraud strategy;
- **Article 45(12):** In the event of any illegal activity, fraud or corruption which may harm the interests of the Union, a member of staff or other servant, including national experts seconded to the Agency, should inform their immediate superior, the Executive Director (ED) or the MB or the European Anti-Fraud Office (OLAF) or the European Public Prosecutor's Office (EPPO) directly. Contracts with external auditors carrying out audits of the financial management of the Agency should provide for an obligation of the external auditor to inform the ED or, if the latter may be



involved, the MB of any suspected illegal activity, fraud or corruption that may harm the interests of the Union;

- **Article 86:** The Agency should inform the Commission without delay on cases of presumed fraud and other financial irregularities. Moreover, it should inform the Commission of any completed or ongoing investigations by the EPPO or OLAF, and of any audits or controls by the European Court of Auditors (ECA) or the Internal Audit Service ('IAS'), without endangering the confidentiality of the investigations.

The EUAA's internal control framework, specifically internal control principle 8, requires the Agency to consider the potential for fraud when assessing risks to the achievement of objectives and to set up and implement measures to counter fraud by putting in place a sound anti-fraud strategy to improve prevention, detection and conditions for investigating fraud, and to set out reparation and deterrence measures, with proportionate and dissuasive sanctions.

5. Fraud and the motives behind it

5.1. Fraud

The concept of fraud encompasses not only acts or omissions that infringe the European Union's (EU) financial interest, but also misconduct.

It covers a range of *irregularities, illegal acts and, infringement of provision of community law* (breach of law) and misconduct characterised by *intentional deception or intent to gain undue advantage*. As portrayed in Figure 1 below, the three main elements that distinguish **fraud** from **irregularity** (error) are: *intent, deception and gain*. In principle, the step up from "irregularity" to "fraud" is made following (professional) investigation where **intent, deception or undue advantage** have been proven. Ultimately, the detection of fraud means the detection of facts or highly suspicious circumstances that suggest fraud may be taking place.

Based on the Commission's AFS, the Agency's AFS will focus on protecting the Agency's (and EU's) financial interests from fraud, corruption, and other intentional irregularities and from any serious wrongdoing. For the purposes of this Internal Guidance and the Agency's AFS, the term 'fraud' should be understood in a broad sense, encompassing:

- fraud, corruption, and misappropriation affecting the EU's financial interests, as defined in Articles 3 and 4 of Directive (EU) 2017/1371²;
- other criminal offences affecting the Union's financial interests, e.g., offences linked to an abuse of procurement procedures where they affect the EU budget;
- irregularities as defined in Article 1(2) of Regulation (EC, Euratom) No 2988/95³ (insofar as they are intentional but not already captured by the criminal offences referred to above);

² Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, (OJ L 198, 28.7.2017, p. 29).

³ Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities' financial interests, (OJ L 312, 23.12.1995, p. 1).

- serious breaches of professional obligations by staff members, as referred to in Article 1(4) and in the second subparagraph of Article 2(1) of the OLAF Regulation.

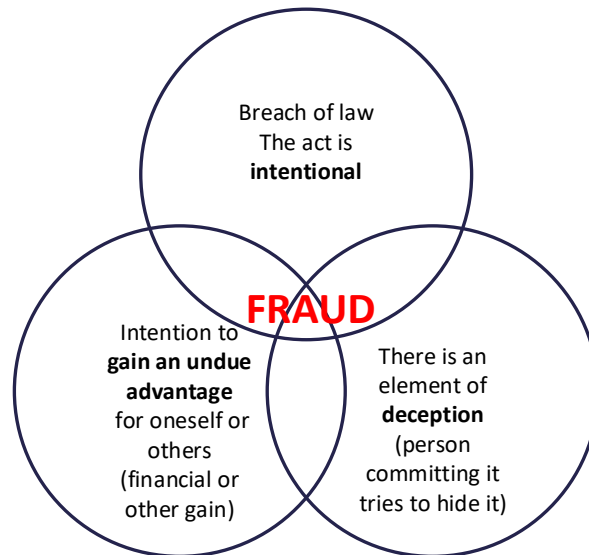


Figure 1: The three main elements of fraud.

5.2. The fraud triangle - opportunity, incentive, and rationalisation

There are three interrelated elements that enable someone to commit fraud:

- **Opportunity:** Fraud is more likely to arise where there is a weak internal control system (e.g., poor detective/preventive controls in place), little fear of exposure and likelihood of detection, or unclear policies with regard to acceptable behaviour;
- **Pressure/motivation:** This is typically based on either greed or need. It might be a real financial need, such as high debts, or it could be a perceived financial need, such as a person who has a desire for material goods but not the means to get them. The motivational factors can also be non-financial. There may be high pressure for good results at work or a need to cover up someone's poor performance;
- **Rationalisation:** Many people obey the law because they believe in it and/or are afraid of being shamed or rejected if they are caught. However, others may be able to rationalise fraudulent actions as:
 - necessary – especially when done for the business;
 - harmless – because the organisation is large enough to absorb the impact;
 - justified – because 'I deserve it, as I work hard and I am underpaid' or 'I was mistreated'.

The three elements are depicted in the fraud triangle (see Figure 2).

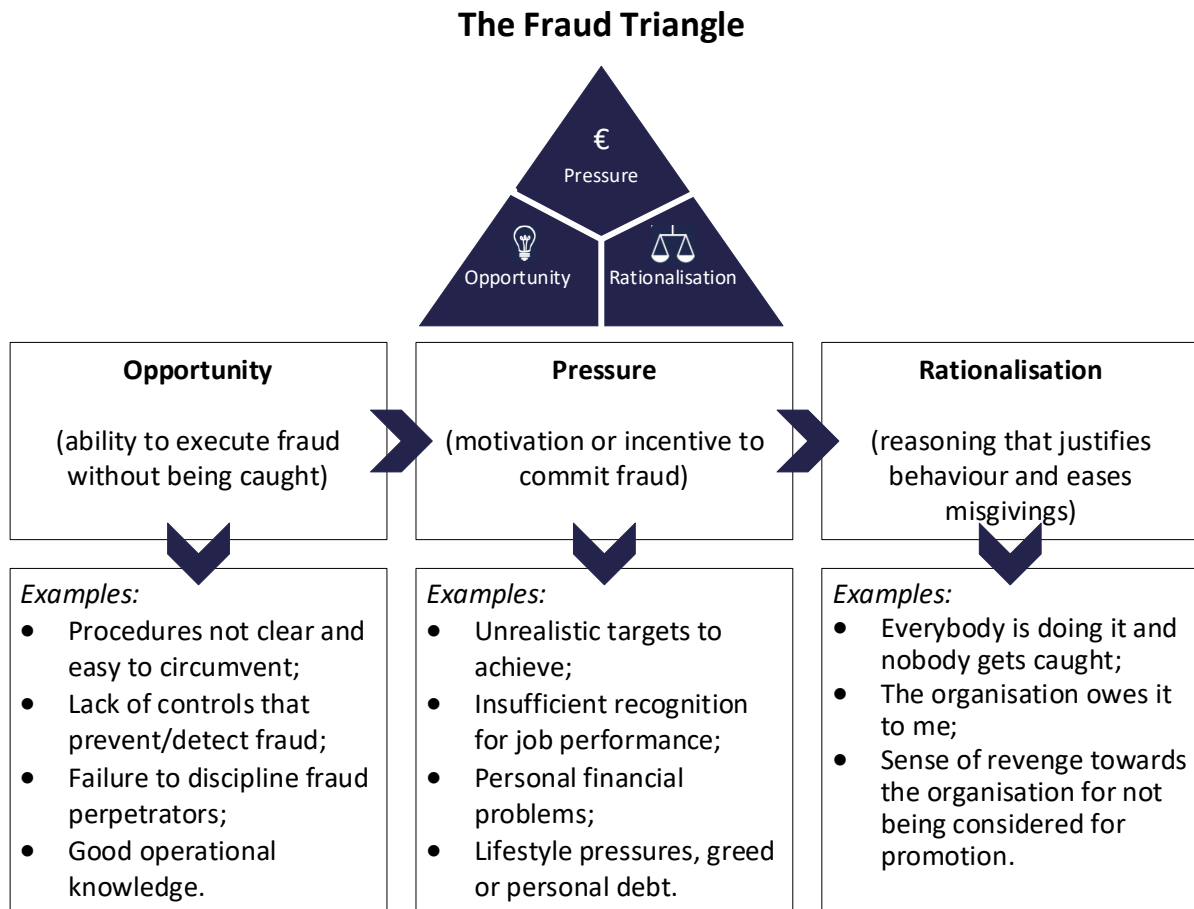


Figure 2: The fraud triangle.

5.3. Reporting on and dealing with suspected fraud

Fraud is intentional, which makes it more difficult to be detected than other irregularities. Those who commit fraud do everything they can to remain undetected. Fraud indicators (or red flags) are distinct signs that fraudulent activity may be taking place and that require immediate attention for management to decide what action is required. Examples of fraud indicators are included in Annex 1.

A key element of prevention and detection of fraud is the establishment and promotion of clear reporting mechanisms. The Agency has developed whistleblowing guidelines to facilitate the safe reporting of both suspicions of fraud and also control weaknesses that may increase the susceptibility to fraud. When a staff member becomes reasonably concerned about such matters, they are encouraged to follow the guidelines outlined in Figure 3.



DO	DO NOT
<ul style="list-style-type: none"> ✓ Read carefully the rights and obligations for whistleblowing that are specified in the whistleblowing guidelines Voice your concern using the normal chain of hierarchical command, i.e., ✓ inform the immediate superior, the ED, or the MB of the Agency, or OLAF or EPPO directly 	<ul style="list-style-type: none"> ✗ Directly accuse the person(s) involved ✗ Investigate on your own ✗ Assume someone else has reported it

Figure 3: What to do in case fraud red flags are identified.

The EUAA’s whistleblowing guidelines specify the different reporting channels that staff members can use to raise a concern or report on suspected fraud or irregularity. Moreover, dedicated whistleblowing channels (e.g., whistleblowing hotlines, anonymous fraud allegation online forms, etc.) are also prominently featured on the [intranet site](#) of the Internal Control and Compliance Unit (ICCU). Any reports received are treated confidentially in accordance with the whistleblowing guidelines.

Based on the Agency’s administrative inquiries and disciplinary proceedings⁴, and in accordance with the EPPO Regulation (particularly Recital 51), the Legal Services Unit (LSU) may perform a preliminary evaluation to determine if an internally reported allegation or a possible case of fraud has prima facie grounds for a further, more thorough investigation and/or for a potential criminal offence against the EU budget. This will be a preliminary assessment phase that is independent from the whistleblowing facilities provided to staff. During the preliminary assessment, all Units are expected to promptly provide LSU with any requested information and/or documents. At the end of the preliminary assessment, LSU shall draw up an assessment note for the ED to decide whether the case is to be closed without further action or warrants a follow-up and referral to OLAF and/or the EPPO.

Furthermore, in accordance with Article 86 of the Agency’s Financial Regulation, the Agency shall inform⁵ the Commission without delay on cases of presumed fraud and other financial irregularities, as well as any completed or ongoing investigations by the EPPO or OLAF, and of any audits or controls by the ECA or the IAS, without endangering the confidentiality of the investigations.

6. Fraud risk management process

6.1. Overview

The Agency adopts a comprehensive approach to fraud management that essentially follows the same methodology for its Agency-wide risk management process.

⁴ IG-006: Internal guidance on administrative inquiries and disciplinary proceedings.

⁵ The ED will inform the Commission either at a MB meeting or through the EUAA’s OLAF correspondent.



When addressing fraud risk as part of an existing risk management exercise, it is possible that the opportunities for fraudulent misrepresentation of financial and non-financial information, misappropriation of assets or misconduct are not adequately examined and identified. Thus, a more targeted approach on managing fraud risk needs to be implemented to provide greater assurance that the Agency’s focus remains on intentional acts.

As depicted in Figure 4, fraud risk management involves the following main steps:

- identifying the fraud risk management objectives and the related priority measures;
- performing a comprehensive fraud risk assessment exercise;
- developing an anti-fraud strategy that defines the control activities to be implemented to mitigate the identified fraud risks;
- establishing corrective actions (including fraud reporting mechanisms and a coordinated approach for the conduct of investigations);
- monitoring and assessing the fraud risk management process to ensure that its outcome supports and is consistent with the overall internal control framework.



Figure 4: A cyclical comprehensive fraud risk management process

The approach that the Agency takes in carrying out each of the main steps outlined in Figure 4 is detailed in Sections 6.2 to 6.4 below. A process map illustrating how these events would unfold in practice and the main actors involved is available [here](#).



6.2. Fraud risk management objectives and priority measures

The Agency has established **five fraud risk management objectives** to enable the identification and assessment of incentives, pressures, opportunities and attitudes which may lead to any type of fraud. These five objectives fully support, are completely consistent with, and complement the 17 internal control principles and five components of the EUAA’s internal control framework (as shown in Table 1).

A set of priority measures are also proposed for each fraud risk management objective as shown in Table 2. These priority measures are intended to assist management in the design, implementation and delivery of fraud risk management activities. However, when developing or revising the AFS, senior management⁶ (SM), upon a proposal of the ICCU, may determine that some of these priority measures are not suitable or relevant and may identify and consider others based on the outcome of the fraud risk assessment and/or the specific circumstances of the Agency.

Table 1: Relationship between the EUAA’s internal control framework and the fraud risk management objectives.

Internal control components and principles		Fraud risk management objectives
Control environment	1. The Agency demonstrates a commitment to integrity and ethical values.	1. Fraud risk governance The SM and MB demonstrate in their instructions and actions a commitment to high integrity and ethical values regarding the management of fraud risk by establishing and communicating to all staff a sound and solid ethical framework and anti-fraud strategy.
	2. The MB demonstrates independence from management and exercises oversight of the development and performance of internal control.	
	3. Management establishes, with political oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
	4. The Agency demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
	5. The Agency holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
Risk assessment	6. The Agency specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	2. Fraud risk assessment Based on the EUAA’s fraud risk management objectives and priorities, the SM performs a comprehensive fraud risk assessment to identify specific fraud incentives, pressures, and
	7. The Agency identifies risks to the achievement of its objectives across the organisation and analyses risks as a basis for determining how the risks should be managed.	

⁶ As defined in Article 5 of the Decision of the Executive Director No 28 of 20 February 2023 implementing Management Board Decision No 127 of 13 February 2023 establishing the Agency’s internal structures, and laying down the internal rules of procedure (ISROP)



	Internal control components and principles	Fraud risk management objectives
	8. The Agency considers the potential for fraud in assessing risks to the achievement of objectives.	opportunities, assess existing fraud control activities and implement actions to mitigate residual fraud risks.
	9. The Agency identifies and assesses changes that could significantly impact the internal control system.	
Control activities	10. The Agency selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	3. Fraud control activity The EUAA mitigates the risk of fraud events occurring or not being detected in a timely manner through selecting, developing, and deploying preventive and detective fraud control activities across all the priority areas.
	11. The Agency selects and develops general control activities over technology to support the achievement of objectives.	
	12. The Agency deploys control activities through corporate policies that establish what is expected and in procedures that put policies into action.	
Information & communication	13. The Agency obtains or generates and uses relevant quality information to support the functioning of internal control.	4. Fraud investigation and corrective action The EUAA establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.
	14. The Agency internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
	15. The Agency communicates with external parties about matters affecting the functioning of internal control.	
Monitoring activities	16. The Agency selects, develops, and performs ongoing and/or separate assessments to ascertain whether the components of internal control are present and functioning.	5. Fraud risk management monitoring activities The EUAA selects, develops, and performs ongoing assessments to ascertain whether each of the five fraud risk management objectives are present and functioning, and communicates the anti-fraud strategy action plan in a timely manner to parties responsible for taking corrective action, including the SM and MB.
	17. The Agency assesses and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including the MB and SM, as appropriate.	



Table 2: Proposed priority measures for each fraud risk management objective.

Fraud risk management objectives	Priority measures
<p>1. Fraud risk governance The SM and MB demonstrate in their instructions and actions a commitment to high integrity and ethical values regarding the management of fraud risk by establishing and communicating to all staff a sound and solid ethical framework and anti-fraud strategy.</p>	<p>1.1. Makes an organisational commitment to fraud risk management With the support of the ICCU, the SM demonstrates a commitment to and is involved in the fraud risk management process by establishing and documenting objectives and priority measures to prevent and detect fraud.</p>
	<p>1.2. Supports fraud risk governance The SM supports fraud risk management as a ‘key element’ of corporate governance by sponsoring and communicating the fraud risk register to the MB and the EUAA’s staff⁷.</p>
	<p>1.3. Establishes a comprehensive anti-fraud strategy and ensures its update The SM provides a solid foundation for fraud risk management by establishing a “comprehensive” anti-fraud strategy. The SM ensures that the anti-fraud strategy is fully documented and revised every 3 years.</p>
	<p>1.4. Establishes fraud risk governance roles and responsibilities across the Agency The SM identifies and appoints the functions with key roles and responsibilities for the implementation of the anti-fraud strategy .</p>
	<p>1.5. Communicate the anti-fraud strategy at all levels The SM supports the ongoing effectiveness of the anti-fraud strategy by maintaining a continuous focus and communicating on fraud deterrence, prevention and detection across the Agency.</p>
<p>2. Fraud risk assessment Based on the EUAA’s fraud risk management objectives and priorities, the SM performs a comprehensive fraud risk assessment to identify specific fraud incentives, pressures and opportunities, assess existing fraud control activities and implement</p>	<p>2.1. Involves appropriate levels of management and staff from across the different units and functions of the Agency The fraud risk assessment process includes managers and staff at relevant levels and recognises that fraud can happen at any level or in any entity of the Agency.</p>
	<p>2.2. Analyses internal and external factors The fraud risk assessment process considers both internal and external factors and their impact on the achievement of objectives.</p>
	<p>2.3. Considers various types of fraud The Agency considers a wide range of possible fraud schemes, and specifically the risk of management overriding controls.</p>

⁷ In the broadest sense without distinction by grade or function: statutory staff (i.e., temporary agents and contract agents), seconded national experts (SNEs), other personnel whose employment contracts are governed by private law, i.e., temporary agency workers (i.e., interims) and other personnel of subcontractors working in the EUAA’s buildings and offices. (Adapted from the OLAF’s definition at [Investigations relating to EU staff \(europa.eu\)](https://www.europa.europa.eu/press_corner/news/2017/04/olaf_definition_en).)



Fraud risk management objectives	Priority measures
<p>actions to mitigate residual fraud risks.</p>	<p>2.4. Estimates the likelihood and significance of identified risks The Agency carefully assesses the probability of occurrence of each particular fraud risk and its potential effects on the Agency if it were to occur.</p>
	<p>2.5. Assess personnel or entities involved and all aspects of the fraud triangle The Agency focuses on incentives and pressures, opportunities, attitudes, and rationalisations to commit fraud.</p>
	<p>2.6. Identifies existing fraud control activities and assesses their effectiveness The fraud risk assessment team identifies and assesses existing and missing controls for effectiveness to determine residual fraud risks that require mitigation.</p>
	<p>2.7. Determines how to respond to risks The fraud risk assessment team’s ultimate goal is to formulate effective and appropriate responses to all fraud risks.</p>
	<p>2.8. Performs periodic reassessments and assesses changes to fraud risk The Agency repeats the risk assessment process periodically and at least once per year and considers changes affecting the EUAA, including changes in the external environment, business operations, staff, and leadership that can impact fraud risks.</p>
<p>3. Fraud control activity The EUAA mitigates the risk of fraud events occurring or not being detected in a timely manner through selecting, developing, and deploying preventive and detective fraud control activities across all the priority areas.</p>	<p>3.1. Promotes fraud deterrence through preventive and detective control activities The Agency addresses its fraud deterrence as a process of eliminating those factors that may cause fraud to occur and understand that deterrence results from having effective preventive and detective fraud control activities in place.</p>
	<p>3.2. Integrates with the fraud risk assessment The Agency ensures that the design and implementation of fraud control activities link directly to the fraud risk assessment.</p>
	<p>3.3. Considers the application of control activities to different levels of the Agency The EUAA ensures that fraud control activities exist across the Agency at all the appropriate levels.</p>
	<p>3.4. Uses a combination of fraud control activities The Agency ensures that fraud control activities include a range, variety and mix of preventive and detective controls that also address the possibility of management overriding controls.</p>
	<p>3.5. Deploys control activities through policies and procedures</p>



Fraud risk management objectives	Priority measures
	The EUAA ensures that fraud control activities are well documented and implemented through policies and procedures.
<p>4. Fraud investigation and corrective action</p> <p>The EUAA establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.⁸</p>	<p>4.1. Establishes fraud investigation and response protocols</p> <p>The Agency establishes processes for communication relating to potential fraud.</p>
	<p>4.2. Conducts investigations</p> <p>The Agency has in place the means to undertake investigations of potential fraud, giving due consideration to the scope, severity, credibility and implications of communicated matter.</p>
	<p>4.3. Takes timely corrective action</p> <p>The Agency selects transparent corrective measures and particularly discipline, remediation, asset recovery, training, civil action and/or criminal referral to address in a timely manner the findings of the investigation.</p>
<p>5. Fraud risk management monitoring activities</p> <p>The EUAA selects, develops, and performs ongoing assessments to ascertain whether each of the five fraud risk management objectives are present and functioning and communicates the anti-fraud strategy action plan in a timely manner to parties responsible for taking corrective action, including the SM and MB.</p>	<p>5.1. Considers a mix of ongoing and separate assessments</p> <p>The SM includes a combination of ongoing and annual monitoring processes to assess whether the fraud risk management objectives and priority measures were effectively achieved.</p>
	<p>5.2. Establishes appropriate measurement criteria</p> <p>The SM establishes appropriate measurement criteria to assist in the objective assessment of its anti-fraud strategy.</p>
	<p>5.3. Assesses, communicates and remediates deficiencies</p> <p>The SM assesses the results of the fraud risk management monitoring programme, communicates deficiencies to those tasked with implementing corrective actions and ensures that appropriate remediation is implemented promptly.</p>

6.3. Fraud risk assessment

6.3.1. Scope and frequency

Within the context of the EUAA’s internal control framework, fraud risks are a subset of the risks that management must assess. Moreover, in accordance with the EUAA’s risk management framework, when conducting the annual risk assessment exercise, each risk shall be analysed in terms of its fraud

⁸ This is dependent on the communication by OLAF or other investigators of the results of their investigation to the appropriate internal authority, and where necessary to external third parties. The EPPO and OLAF are bound to conduct investigations in a timely and effective manner.



potential (i.e., fraud filter). Thus, unless there is a justifiable reason, fraud risks must be identified and managed as part of the general risk assessment process, which is a cyclical process that is linked with the single programming document cycle and is organised at least once per year.

However, while the development or updating of the EUAA's AFS may take advantage of possible synergies and rely partially on the annual risk assessment results, the Agency should ensure that, when developing an AFS, as well as in the years when an update is due, a specific, fully-fledged fraud risk assessment is conducted using the methodology outlined in this Internal Guidance. Overall, conducting a specific, comprehensive fraud risk assessment exercise will help the Agency to better understand its fraud risks, develop targeted controls to prevent and detect fraud, enhance compliance, and build a strong anti-fraud culture.

6.3.2. Identifying fraud risks

The EUAA's risk management framework defines a risk as "any event or issue that could occur and adversely impact the achievement of the Agency's political, strategic and operational objective." A risk always relates to the non-achievement of an objective and should be formulated in terms of cause and potential consequence.

A risk of fraud exists particularly when there is a serious weakness, or a combination of deficiencies, in a process that may give rise to potential fraud. Fraud can involve both financial and non-financial risks, such as reputational impact. Sometimes, the reputational impact of fraud exceeds the financial cost.

Since fraud risk assessment forms the basis of the Agency's AFS, when identifying fraud risks, the notion of fraud should not be restricted to its criminal meaning, but should be considered in a broader context as described in Section Fraud5.1 above. Furthermore, when considering that the motives for committing fraud are numerous and diverse, the fraud risk identification process should include an assessment of the incentives, pressures, and opportunities to commit fraud. Annex 2 provides a non-exhaustive list of potential types of fraud (internal or external) that may be considered when carrying out the fraud risk assessment.

The fraud risk assessment is coordinated by the ICCU that may use any or all of the following three approaches when identifying fraud risks:

- high level review;
- targeted review, and/or
- bottom-up perspective.

It is good practice to combine all these approaches when conducting a fraud risk assessment. The following sources of information may have valuable data that can be referred to in order to help identify such risks:

- central risk register (significant/critical risks) and Units' risk registers (low and medium risks);
- audit reports of the ECA and the IAS;
- internal and external evaluation reports;
- results of monitoring, *ex ante* and *ex post* controls;
- central register of internal control deficiencies and corrective action plan;
- training sessions on anti-fraud;



- material from the OLAF, e.g., final case reports, OLAF casebooks, training material, strategic analysis reports;
- potential cases of fraud identified and reported by *ex post* controllers, the ECA, the IAS or other control bodies in the context of an audit;
- internal surveys;
- knowledge and experience of staff members (which can be tapped into, e.g., by organising seminars, information sessions, workshops or interviews).

The fraud risk assessment questionnaire in Annex 3 includes a set of model questions that could be replied to by various internal stakeholders to assist the ICCU and SM in identifying fraud risks. This questionnaire can be modified by the ICCU to align it to the specific circumstances of the Agency and ensure that it remains relevant and effective over the years in identifying potential fraud risks. Any changes to the questionnaire will be reviewed by the Deputy ED before they are presented for discussion and endorsement by the SM.

6.3.3. Assessing the likelihood and impact

During this phase of the process, the severity of the fraud risk is assessed. All fraud risks cannot be handled at the same time; some of them may have a greater impact or a greater likelihood of occurring and therefore require a more specific response. A fraud risk should be prioritised depending on its potential impact and the likelihood of its occurrence, both assessed on a five-point scale, ranging from 1 (very low impact, low likelihood) to 5 (very high impact, extremely likely). This assessment should follow the guidance provided in the EUAA's risk management framework.

The assessment of a fraud risk shall focus on the residual risk (i.e., the risk that remains after having considered the controls that have already been put in place). Depending on the effectiveness of the internal control system in place in the Agency, the likelihood of occurrence of a fraud might be very low. The main aspect to focus on when assessing the fraud risk is the impact and the extent of the damage. The impact may be reputational, financial, or operational in nature. The model questions included in fraud risk assessment questionnaire (Annex 3) are also designed to assist in assessing which controls are in place or should be in place to mitigate the identified fraud risks.

It is not possible to entirely prevent fraud from happening, but it is possible to adopt a zero-tolerance approach towards fraud. In particular, an assessment should be made as to whether the actors within the Agency and the tools at their disposal are appropriate to address the identified risks. The risk response to an identified risk of fraud (which must be addressed in the anti-fraud strategy) should be proportionate, quick and of great attention.

The severity of the identified fraud risks and the risk responses are proposed by ICCU on the basis of the internal stakeholders' input to the fraud risk assessment questionnaire and the information gathered from the sources outlined in section 6.3.2.

The preliminary results of the fraud risk assessment exercise are discussed with the risk management correspondents before being reviewed by the Deputy ED. The proposed significant and critical fraud risks must be reported to and re-assessed by the SM that will also determine how to respond to these fraud risks, consider how each risk should be managed, and whether to accept, avoid, reduce or share the risk. In most cases, the risk should be managed by reducing it through an adequate control measure.



6.3.4. Monitoring of fraud risks

Once fraud risks have been identified and assessed, they are registered by the ICCU in a specific fraud risk register, which is monitored on a quarterly basis along with the central risk register that includes the significant/critical risks identified and prioritised in the annual risk management exercise. This allows regular monitoring of the risks and ensures completeness of the Agency's risk profile. Moreover, the risk response for the critical and significant fraud risks will be documented in the Agency's AFS, and detailed in an action plan to be implemented, monitored, and reported on as further described in Section 6.4.4. below.

6.4. Anti-fraud strategy

6.4.1. Scope of the anti-fraud strategy

The outcome of the fraud risk assessment exercise should be a robust Agency AFS, intended to provide a framework for addressing the subject of fraud at an Agency-wide level. The drafting of the anti-fraud strategy gives the Agency an opportunity to reflect on the extent of fraud risks it faces when carrying out its activities, the types of measures that are already in place and what other measures need to be introduced to mitigate further risks of fraud.

The AFS shall define the priority measures that will help the Agency in achieving the pre-defined fraud risk management objectives that are linked to the Agency's internal control framework, as described in Section 6.2, as well as in addressing the identified critical and significant fraud risks. The AFS should also be accompanied by an action plan with measurable indicators (where possible) that reflects the priorities established by the Agency and describes the risk responses and control activities that must be implemented to mitigate those fraud risks.

The AFS and the corresponding actions are to be embedded in the Agency's internal control system and should take into account the principle of cost effectiveness and proportionality. Based on OLAF's AFS methodology guidance document, it is recommended that the Agency's anti-fraud strategy and actions:

- be designed with the objectives of the Commission's anti-fraud strategy in mind, especially in developing anti-fraud activities, particularly through improving prevention, detection, the conditions for investigating fraud (including closer cooperation with the OLAF), and awareness raising;
- encompass all stages of the anti-fraud cycle, i.e., not only through prevention and detection but also by way of investigations and recovery/sanctions. Swift exchange of key information and full cooperation between the OLAF and the Agency during the investigation will facilitate the work of both bodies and may help the Agency take decisions and/or precautionary measures. Apart from recovery, a high level of reactivity and relevance of the action taken acts as a strong deterrent. Reactivity is critical at each stage of the anti-fraud cycle. The Agency should consider how its internal procedures will respond if a potential fraud is detected. Fraud cases should lead to a criminal conviction. Thus, there should be no delay in taking any of the administrative steps required (including reporting to the OLAF) that could allow the fraudster to avoid a sentence.



A draft (or an update) of the AFS is to be proposed by the ICCU based on the methodology provided in this Internal Guidance and the outline content headings provided in Annex 4. The proposed draft will be reviewed by the Deputy ED before being presented to the SM and ED for discussion and endorsement. The final draft must be approved and adopted by the MB.

The SM are to be involved in the development or revision of the AFS to leverage their expertise and ensure ownership and acceptance of the strategy. Furthermore, as specified in the OLAF's AFS methodology guidance, given that OLAF has built up extensive knowledge of fraud patterns, fraud indicators and so on in carrying out its missions, the Agency should request the OLAF's assistance to make an informal/formal contribution to the drafting of the AFS. Prior to approval of the Agency's AFS by the ED and adoption by the MB, ICCU will also solicit input from the Commission's Directorate-General for Migration and Home Affairs (DG HOME) on the proposed draft AFS.

6.4.2. Preparing the action plan to implement the anti-fraud strategy

The action plan should clearly link the priority measures with actions, actors, deadlines, and indicators (where possible). The Agency has a wide range of tools at its disposal for combating fraud, allowing it to develop effective and efficient actions. Consideration may be given to the following areas:

- management: setting the tone at the top, training, follow-up, seminars;
- staff: fraud awareness, anti-fraud culture, training, meetings;
- development and use of IT tools;
- development of guidelines for staff on how to react when facing a potential case of fraud;
- improving clarity of wording of templates for contracts, agreements, decisions, notifications;
- monitoring, e.g., specific checks, reports to managers, etc.

At the outset, the Agency must develop a set of anti-fraud control objectives to address the most significant and critical fraud risks identified. The objectives must be realistic and achievable and integrated into the day-to-day business operations of the Agency. In addition, for all significant and critical fraud risks, at least one corresponding control activity or measure should be inserted. At this stage, cost-benefit considerations and the availability of human resources become a key issue, thus leading the Agency to concentrate efforts on implementing key control activities, whilst postponing others. It may be possible that one action covers several risks. If this is the case, this should be clearly defined in the action plan. Gaps between the fraud risk assessment and the action plan should be fully explained.

The fraud risk register action plan should be annexed to the Agency's AFS and include the headings set out in Annex 5.

6.4.3. Establishing related indicators and targets

Performance indicators are key elements that may help monitor the progress made in the implementation of the action plan and in the attainment of objectives. In this regard, the Agency may identify which of the performance indicators that are already in use as part of the internal control self-assessment can be used for reporting on the Agency's AFS and help assess the impact of the implementation of the strategy.



6.4.4. Assessing and updating the anti-fraud strategy and/or the related action plan

Strategies should normally remain stable unless important developments within the Agency (e.g., re-organisation or new mandate) or the policy area call for an update. After the first-time adoption of an anti-fraud strategy, based on the recent Commission AFS methodology and guidance, the Agency should in principle update its AFS every three years following adoption by the MB. Nevertheless, the action plan may be updated more frequently than the AFS.

The action plan and, where appropriate, the AFS shall be updated on the basis of an evaluation of the impact of the strategy, measured using the indicators set in Section 6.4.3, as well as of its effectiveness, efficiency, relevance and coherence. To that end, it must be determined to what extent:

- the activities and deadlines set out in the action plan have been adhered to;
- the results of the implementation of the strategy correspond to the objectives set out therein.

The ICCU will be monitoring the fraud risks and the implementation status of the action plan on a quarterly basis (see Annex 5 for the status reporting heading to be added to the action plan). The preliminary results of the monitoring exercise will be reviewed by the Deputy ED before being presented for endorsement to the ED. Following which, the ICCU will report to the MB at plenary meetings on the implementation status of the action plan, any new fraud risks and/or new actions required. On an annual basis, through the consolidated annual activity report, the ED will also report to the MB on the overall progress of the AFS and its action plan.

6.4.5. Disclosing and communicating the anti-fraud strategy

As required by Article 32 of the Agency's Financial Regulation, the single programming document must contain information on a strategy for the organisational management and internal control systems including the AFS as last updated and an indication of measures to prevent recurrence of cases of conflict of interest, irregularities, and fraud.

The consolidated annual activity report is also required in accordance with Article 48 the Agency's Financial Regulation to include information on organisational management and on the efficiency and effectiveness of the internal control systems including the implementation of the AFS.

The Agency will make the AFS and a summarised version of the action plan publicly available on its website as part of its efforts to foster a culture of transparency and accountability. Due to the sensitivity and confidentiality of the information included within, the detailed results of the fraud risk assessment must be documented separately from the AFS, necessitating also restricted access.

The EUAA's AFS and a summarised version of the accompanying action plan must also be disseminated internally to help raise staff awareness and continue strengthening the anti-fraud culture within the Agency.

The OLAF should be notified whenever an AFS is adopted and provided with a copy of the document.



7. Summary of changes







Version no.	Changes
01	New IG. Complete re-write of EASO/EDD/2020/78.



Annex 1: Examples of fraud indicators (or red flags)




1. Undisclosed conflict of interest

A conflict of interest exists when an actor's impartial and objective performance of their tasks is compromised for reasons involving family, emotional life, political or national affinity, economic interest or any other shared interest with a recipient. The threat comes from conflicts of interest that are not disclosed. When a conflict of interest is acknowledged, it can be managed and mitigated in an appropriate manner.

-  Unexplained or sudden increase in wealth not justified by the salary received.
-  Unexplained or unusual favouritism to a particular contractor.
-  Continued acceptance of high-priced, low-quality work etc.
-  Refuse to take up a new post because of links created in the old one.
-  Failure to file or complete conflict of interest declaration.
-  Undisclosed outside business.




2. Unjustified single source awards

This scheme often results from corruption, especially if the pattern is repeated and questionable. Such awards can be made by splitting purchases to avoid competitive procedure thresholds, falsifying single source acquisition justification, drafting very narrow specifications, extending previously awarded contracts rather than re-tendering.

-  Single source awards above or just below competitive procurement thresholds.
-  Previously competitive procurements become non-competitive.
-  Request for services mailed only to one service provider.

3. Split purchases

A purchase may be split 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 can indicate corruption or other fraudulent activity.

-  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.

4. Rigged specifications

Requests for offers or calls for tenders might contain specifications tailored to meet the qualifications of a particular tenderer, or which only one tenderer can meet. Specifications which are too narrow can be used to exclude other qualified tenderers, or to justify single source acquisitions and avoid competition altogether. A pattern of rigged specifications which favour a particular contractor suggests corruption.

-  Only one or a few tenderers respond to request for bids.



- ⌘ Similarity between specifications and winning contractor's product or services.
- ⌘ Complaints from other tenderers.
- ⌘ Specifications are significantly narrower or broader than similar previous requests for offers.
- ⌘ Unusual or unreasonable specifications.
- ⌘ High number of competitive awards to one supplier.
- ⌘ Socialisation or personal contacts between staff members and tenderers during the tender submission process.
- ⌘ Specifications define an item using brand name rather than generic description.

5. Leaking of information

Confidential information is leaked to help a favoured economic operator formulate a technical or financial offer, such as estimated budgets, preferred solutions, or the details of competing offers.

- ⌘ Winning offer just under the next lowest offer.
- ⌘ Some tender offers opened early.
- ⌘ Acceptance of late tender offers.
- ⌘ All offers are rejected and contract is re-tendered.
- ⌘ Winning tenderer communicates privately with procurement officer by e-mail or otherwise during the tender submission period.

6. Manipulation of offers

Offers are manipulated after receipt to ensure that a favoured contractor is selected (changing bids, "losing" bids, voiding bids for alleged errors in specifications, etc.).

- ⌘ Complaints from tenderers.
- ⌘ Poor controls and inadequate procurement procedures.
- ⌘ Indications of changes to offers after reception.
- ⌘ Tender offers voided for errors.
- ⌘ A qualified tenderer disqualified for questionable reasons.
- ⌘ Job not re-tendered even though fewer than the minimum number of offers were received.

7. Collusive bidding

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

- ⌘ Winning offer is too high compared to cost estimates or industry averages.
- ⌘ Persistent high prices by all tenderers.
- ⌘ Unusual tender offer patterns (e.g., offers are exact percentage apart, winning offer just under threshold of acceptable prices, etc.).
- ⌘ Apparent connections between tenderers, e.g., common addresses, phone numbers, etc.
- ⌘ Tenderer includes subcontractors in its offer which are competing for the main contract.
- ⌘ Qualified contractors fail to tender and become subcontractors or low tenderer withdraws and becomes a subcontractor.

8. Unbalanced bidding

Favoured tenderer may be provided with useful inside information, for example, that one or several line items in a request for offer will not be used in the contract (some line items may also be vague or ambitious on purpose and the favoured tenderer is instructed how to respond). This



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

- Ⓜ Particular line-items in the offer appear to be unreasonably low.
- Ⓜ Changes are issued soon after contract awards to delete or modify line-item requirements.
- Ⓜ Line-items for tender offers are different than the actual contract.

9. Cost mischarging

A contractor can commit fraud by intentionally charging costs which are not allowable or reasonable, or which cannot be allocated, directly or indirectly, to a contract. Labour costs can be manipulated by creating fictitious timesheets, altering timesheets or invoicing for inflated labour costs without supporting documentation.

- Ⓜ Excessive or unusual labour charges.
- Ⓜ Labour charges inconsistent with contract progress.
- Ⓜ Timesheets cannot be found.
- Ⓜ Same material costs charged to more than one contract.

10. Failure to meet contract specifications

Contractors which fail to meet contract specifications and then knowingly misrepresent that they have met them commit fraud (e.g., use of sub-standard building materials, inferior quality parts, etc. The motive is to increase profits by cutting costs or to avoid penalties for failing to meet deadlines, etc. Such schemes are difficult to detect without close inspections or tests by independent subject matter experts.

- Ⓜ Discrepancy between test and inspection results and contract claims and specifications.
- Ⓜ Absence of test or inspection document or certificates.
- Ⓜ Low quality, poor performance and high number of complaints.

11. False, inflated or duplicate invoices

Contractor might knowingly submit false, inflated or duplicate invoices, either acting alone or in collusion with Agency staff members.

- Ⓜ 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.
- Ⓜ 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.

12. Phantom service provider

This may include for instance payments authorised to a fictitious seller in order to embezzle funds or the setting up of phantom companies by tenderers to submit complementary offers in collusive tendering schemes, to inflate costs or simply to generate fictitious invoices.

- Ⓜ Service provider cannot be found in any directories, internet search engines etc.
- Ⓜ Service providers address cannot be found.



- 🔗 Service provider lists incorrect street address or phone number.

13. Product substitution

This refers to the substitution, without the Agency's knowledge, of inferior quality items for those which are specified in the contract. The substitution often involves component parts which are not easily detected.

- 🔗 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.
- 🔗 Above average operation failures, early replacements, or high maintenance or repair costs.
- 🔗 Compliance certificates signed by unqualified or non-certified persons.
- 🔗 Significant difference between estimated and actual costs for materials.



Annex 2: Examples of fraud activities

The following is a non-exhaustive list of potential types of (internal and external) fraud the Agency may consider when carrying out its fraud risk assessment exercise.

Fraud type	Description
Falsification of documents	<ul style="list-style-type: none"> • An expert submits inflated cost claims by producing false timesheets. • An employee creating false supplier invoices/payment instructions with forged signatures and submitting them for processing. • Improper capitalisation of expenses as fixed assets. • Delaying the recording of expenses to the next accounting period. • Intentional manipulation of financial figures (e.g., misstatement of pre-payments, accruals, etc). • Submission of fraudulent expenditure claims using false receipts to claim travel and accommodation allowances. • Presentation of a false CV to be selected for an open recruitment process. • Presentation of a false report by an external expert to manipulate the results of the study.
Corruption	<ul style="list-style-type: none"> • The abuse of entrusted power for private gain, including bribery.
Plagiarism	<ul style="list-style-type: none"> • Use of internet pages or other texts drafted by another person and claiming to be the author.
Favouritism	<ul style="list-style-type: none"> • The contract specification is written in a manner which favours a particular technical, end user and financial supplier. • Recruiting staff where they not needed. • Recruiting staff who are not qualified. • Purchase not needed ('gold plating'). • Slicing markets to circumvent review/approved limits. • Delaying awarding decision to create time pressure.
Theft or misappropriation of assets/funds	<ul style="list-style-type: none"> • Overcharged invoicing to cover work done in the dwelling of a staff member. • Selling data from the database maintained by the Agency for own profit. • Uncontrolled inventory shrinkage. • Manipulating the bank account to make payment to the wrong entity. • Submission of and reimbursement of ineligible expenditure claims. • Requesting double reimbursement of, e.g., medical expenses, travel allowances, removal expenses.
Leaking of information	<ul style="list-style-type: none"> • Leak of intangible assets (IP, personal data, etc.). • Leak critical tender offers information (or other sensitive technical specifications) to favour specific potential tenderers over others.



Fraud type	Description
	<ul style="list-style-type: none"> Leak of critical information for personal gain or to intentionally damage the reputation of the Agency.
Conflict of Interest	<ul style="list-style-type: none"> Receiving kickbacks from a supplier for treating him favourably during a bidding process. Biased selection and award criteria in the evaluation process to favour a supplier in which a staff member has a financial interest. Management hires a family member over another more qualified applicant.
Collusion	<ul style="list-style-type: none"> Processing false invoices for work not carried out, or inflated invoices for actual work done and in return Agency staff member(s) receive bribes or 'kickbacks' in doing so. Price fixing between potential tenderers to secure business and maximise profit margins.
Other	<ul style="list-style-type: none"> Wilful destruction or removal of records. Concealment of material facts by potential tenderers (e.g., non-declaration of bankruptcy).



Annex 3: Model questionnaire for the fraud risk assessment

For each of the pre-defined fraud risk management objectives and priorities, a series of model questions are presented below. They are based on those provided in the Commission’s AFS methodology and guidance and were reviewed by the OLAF.

The questions are intended to be addressed to the internal stakeholders indicated in the questionnaire. These stakeholders are not always necessarily responsible for the processes/controls under assessment. However, the ICCU may decide to extend the questionnaire to other internal stakeholders, including the scope of the questions.

Internal control principle	Model questions	Internal stakeholders
Fraud risk management objective 1: Fraud risk governance		
The SM and the MB demonstrate in their instructions and actions a commitment to high integrity and ethical values regarding the management of fraud risk by establishing and communicating to all staff a sound and solid ethical framework and anti-fraud strategy		
Priority measure 1.1: Makes an organisational commitment to fraud risk management		
With the support of the ICCU, the SM demonstrates a commitment to and is involved in the fraud risk management process by establishing and documenting objectives and priority measures to prevent and detect fraud.		
1	1.1.1 Does the SM foster the development of an anti-fraud culture (e.g., by ensuring appropriate training on anti-fraud matters, including whistleblowing procedures, for staff, enforce a zero-tolerance approach on fraud issues, etc.)?	HRU/ICCU/SC
1	1.1.2 Are fraud prevention risk management objectives and priority measures defined, updated as needed and approved at the right level of management?	ICCU
1	1.1.3 Is there mandatory training on ethics and integrity, respect, and dignity?	HRU/ICCU/SC
1	1.1.4 Do the Agency's whistleblowing guidelines have a prominent place on the EUAA's intranet site?	HRU/ICCU/SC
1	1.1.5 Is a policy for the prevention and management of conflicts of interest available on the EUAA's website and updated when applicable?	HRU/C1/C2/C3/BSSU/ICCU/SC
1	1.1.6 Are awareness-raising sessions for staff members on the newly implemented policy for the prevention and management of conflicts of interest organised?	HRU/ICCU/SC
1	1.1.7 Is there a system in place for recording details of any arising potential or real conflicts of interest, as well as of any actions taken to address/resolve such conflicts?	HRU/C1/C2/C3/



Internal control principle	Model questions	Internal stake-holders
		EICU/BSSU/ICCU/SC
1	1.1.8 Are declarations of interest of MB members/SM reviewed and/or updated and published annually on the EUAA's website?	HRU/MB Secretariat /ICCU
1	1.1.9 Is there internal guidance available to staff on requests for assistance under Articles 24 and 90 of the Staff Regulations? If so, is this information available to the staff on the EUAA's intranet site?	LSU/ICCU/SC
2	1.1.10 Does the MB monitor the EUAA's management's progress towards pre-defined internal control objectives across key governance areas (incl. fraud prevention)?	BSSU/ICCU
<p>Priority measure 1.2: Supports fraud risk governance</p> <p>The SM supports fraud risk management as a 'key element' of corporate governance by sponsoring and communicating the fraud risk register to the MB and staff⁹.</p>		
2	1.2.1 Are the risk management correspondents (RMC) briefed about fraud prevention and fraud risk management as part of the annual risk management exercise kick-off meeting?	ICCU
<p>Priority measure 1.3: Establishes a comprehensive anti-fraud strategy and its ensures its update</p> <p>The SM provides a solid foundation of fraud risk management by establishing a "comprehensive" anti-fraud strategy. The SM ensures that the anti-fraud strategy is fully documented and revised every three years.</p>		
1	1.3.1 Is the Agency's AFS regularly revised based on a pre-defined fraud risk management methodology?	ICCU
<p>Priority measure 1.4: Establishes fraud risk governance roles and responsibilities across the Agency</p> <p>The SM identifies and appoints the functions with key roles and responsibilities regarding the implementation of the Anti-Fraud Strategy.</p>		
3	1.4.1 Are roles and responsibilities in preventing, detecting and correcting fraud clearly defined?	ICCU
3	1.4.2 Are ethics correspondents formally appointed from the HRU?	HRU/ICCU
3	1.4.3 Are the roles and responsibilities of the ethics correspondents clearly defined and has an adequate training map been developed for them?	HRU/ICCU
3	1.4.4 Are staff informed of the escalation mechanisms for reporting fraud red flags, irregularities, or other serious wrongdoing?	HRU/ICCU/SC

⁹ In the broadest sense without distinction by grade or function: statutory staff (i.e., temporary agents and contract agents), seconded national experts (SNEs), other personnel whose employment contracts are governed by private law, i.e., temporary agency workers (i.e., interims) and other personnel of subcontractors working in the EUAA's buildings and offices. (Adapted from the OLAF's definition at [Investigations relating to EU staff \(europa.eu\)](https://investigations.relativ.to/EU_staff/europa.eu).)



Internal control principle	Model questions	Internal stake-holders
<p>Priority measure 1.5: Communicate the anti-fraud strategy at all levels</p> <p>The SM supports the ongoing effectiveness of the anti-fraud strategy by maintaining and communicating a continuous focus on fraud deterrence, prevention and detection across the Agency.</p>		
1	1.5.1 Is anti-fraud training mandatory for target populations of staff?	ICCU/SC
1	1.5.2 Are lessons learnt from anonymised cases of fraud disseminated to relevant staff through training?	LSU/ICCU
3	1.5.3 How are good practices concerning prevention and detection of fraud exchanged between the centres/units/sectors (e.g., brainstorming, workshops, unit meetings where the cases encountered may be presented and discussed)? How can it be improved?	C1/C2/C3/ICCU/SC
3	1.5.4 How are good practices concerning recovery actions exchanged between the centres/units/sectors? How can it be improved?	C1/C2/C3/ICCU/SC
3	1.5.5 Is the Agency's AFS well communicated and easily accessible to staff and external stakeholders, subject to restrictions regarding confidential information?	FINU/ICCU
5	1.5.6 Is there a process in place that requires newly recruited staff/experts/members of the Consultative Forum to provide a police certificate of conduct, as well as a signed declaration of absence of conflict of interest?	HRU/C1/C2/C3/EICU/ICCU/SC
5	1.5.7 Are background checks on qualifications and employment history for all potential recruits conducted?	HRU/ICCU
5	1.5.8 Does the Agency conduct systematic exit interviews with staff leaving the Agency to identify perceived weaknesses?	HRU/ICCU/SC
5	1.5.9 Are the results of the exit interviews analysed by HRU and the relevant head of unit, and the conclusions presented to the SM?	HRU/ICCU/SC
5	1.5.10 Is the exit interview procedure formalised in line with the governance documents policy (EUAA/EDD/2022/058)?	HRU/ICCU
<p>Fraud risk management objective 2: Fraud risk assessment</p> <p>Based on the EUAA's fraud risk management objectives and priorities, the SM performs a comprehensive fraud risk assessment to identify specific fraud incentives, pressures and opportunities, evaluate existing fraud control activities and implement actions to mitigate residual fraud risks.</p>		
<p>Priority measure 2.1: Involves appropriate levels of management and staff from across the different units and functions of the Agency</p> <p>The fraud risk assessment process includes managers and staff at relevant levels and recognises that fraud can happen at any level or in any entity of the Agency.</p>		



Internal control principle	Model questions	Internal stake-holders
6	2.1.1 Are resources assigned to the EUAA sufficient to achieve the Agency's new mandate and strategic objectives while avoiding any fraud pressure?	C1/C2/C3/ BSSU/ICCU
7 & 8	2.1.2 Is fraud risk assessment an inclusive process across functions, hierarchical levels, services, and projects?	C1/C2/C3/ ICCU
7 & 8	2.1.3 Does the fraud risk assessment involve staff with solid working knowledge of the entire spectrum of functions performed in the Agency?	ICCU
7 & 8	2.1.4 Is there any internal preparation for the risk management correspondents' meetings and does preparation involve the majority of units?	C1/C2/C3/ ICCU
8	2.1.5 Is there cooperation with the OLAF for the preparation of the AFS?	ICCU
7 & 8	2.1.6 Is the procurement risk assessment methodology well defined in terms of scope, frequency, risk tolerance and responsibilities, and is it aligned to the Agency's risk management manual?	PFMU/ ICCU
<p>Priority measure 2.2: Analyses internal and external factors</p> <p>The fraud risk assessment process considers both internal and external factors and their impact on the achievement of objectives.</p>		
7 & 8	2.2.1 Are internal and external factors taken into account during the annual risk assessment exercise (and where applicable during the fraud risk assessment process)?	ICCU
<p>Priority measure 2.3: Considers various types of fraud–</p> <p>The Agency considers a wide range of possible fraud schemes, and specifically the risk of management overriding controls</p>		
7 & 8	2.3.1 Does the fraud risk assessment take into consideration the potential overriding of controls by management, as well as areas where controls are weak or there is a lack of segregation of duties?	ICCU
7 & 8	2.3.2 Are deviations from established controls allowed, approved by the ED and documented in a central register for exceptions?	ICCU
7 & 8	2.3.3 Is the procedure that needs to be followed where responsible authorising officers (RAOs) want to overrule the validation of the verification function duly documented and approved at the right level of management in line with the governance documents policy (EUAA/EDD/2022/058)?	FINU/ICCU
<p>Priority measure 2.4: Estimates the likelihood and significance of identified risks</p> <p>The Agency carefully assesses the probability of occurrence of each particular fraud risk and its potential effects on the Agency if it were to occur.</p>		



Internal control principle	Model questions	Internal stake-holders
7 & 8	2.4.1 Are the identified fraud risks regularly assessed and monitored in line with the fraud risk management methodology and reported to the SM and the MB?	ICCU
<p>Priority measure 2.5: Assess personnel or entities involved and all aspects of the fraud triangle The Agency focuses on incentives and pressures, opportunities, attitudes, and rationalisations to commit fraud.</p>		
8	2.5.1 Are management and staff, particularly those involved in budget implementation, risk management correspondents and <i>ex post</i> controllers, aware of fraud risks and trained to detect and escalate at the appropriate level fraud red flags?	C1/C2/C3/ICCU/SC
8	2.5.2 Are awareness raising measures on fraud prevention and identification, including all aspects of the fraud triangle, documented and made available to staff?	ICCU
8	2.5.3 Has management identified and assessed all potentially sensitive functions that may be highly susceptible to improper conduct or fraud?	ICCU
<p>Priority measure 2.6: Identifies existing fraud control activities and assesses their effectiveness The fraud risk assessment team identifies and assesses existing and missing controls for effectiveness to determine residual fraud risks that require mitigation.</p>		
7 & 8	2.6.1 In assessing the residual fraud risks are the effectiveness/ appropriateness of the existing control activities taken into consideration?	ICCU
<p>Priority measure 2.7: Determines how to respond to risks The fraud risk assessment team's ultimate goal is to formulate effective and appropriate responses to all fraud risks.</p>		
7 & 8	2.7.1 Is information gathered by ICCU during the fraud risk assessment channelled to all units/staff concerned?	ICCU
8	2.7.2 Are the additional remedial actions required to address the resulting fraud risks being implemented in a timely manner by the responsible actors?	ICCU
<p>Priority measure 2.8: Performs periodic reassessments and assesses changes to fraud risk The Agency repeats the risk assessment process periodically and at least once per year and considers changes affecting the EUAA, including changes in the external environment, business operations, staff, and leadership that can affect fraud risks.</p>		
7 & 8	2.8.1 Are periodic re-assessments of the Agency fraud risks conducted taking into account changes impacting the EUAA, such as changes in the external environment, business operations, staff, and leadership, which can affect fraud risks.	BSSU/ICCU



Internal control principle	Model questions	Internal stake-holders
<p>Fraud risk management objective 3: Fraud control activity</p> <p>The EUAA mitigates the risk of fraud events occurring or not being detected in a timely manner through selecting, developing, and deploying preventive and detective fraud control activities through all the priority areas.</p>		
<p>Priority measure 3.1: Promotes fraud deterrence through preventive and detective control activities</p> <p>The Agency addresses its fraud deterrence as a process of eliminating those factors that may cause fraud to occur and understand that deterrence results from having effective preventive and detective fraud control activities in place.</p>		
10	3.1.1 Do fraud prevention awareness training sessions consider how the perpetrators of fraud may try or have tried to circumvent rules, and do they also provide concrete examples that may arise?	ICCU
10	3.1.2 Is the Agency considering fraud risks when it comes to designing and administering grants?	PFMU/ ICCU
10	3.1.3 Is the Agency planning to raise awareness amongst staff members and/or grant beneficiaries on grant-related fraud?	PFMU/ ICCU
10	3.1.4 Are <i>ex ante</i> verifying agents given the code of professional standards that explains amongst other things their mission as verifying agents to support the ED in the achievement of internal control objectives that include fraud prevention and are such staff requested to sign the code as evidence that they have read and understood its provisions?	FINU/ PFMU/ ICCU
10	3.1.5 Is contributing to fraud detection included in the brief for <i>ex post</i> controls carried out by the Agency's <i>ex post</i> controllers? When detecting irregularities do they consider the possibility that fraud has occurred?	ICCU
<p>Priority measure 3.2: Integrates with the fraud risk assessment</p> <p>The Agency ensures that the design and implementation of fraud control activities link directly to the fraud risk assessment.</p>		
10	3.2.1 Is fraud considered in the design and implementation of internal control activities?	FINU/ PFMU/ ICCU
10	3.2.2 Is the design and implementation of fraud control activities linked directly to the identified fraud risks?	ICCU
<p>Priority measure 3.3: Considers the application of control activities to different levels of the Agency</p> <p>The EUAA ensures that fraud control activities exist throughout the Agency at all appropriate levels.</p>		
10	3.3.1 Is there a declaration provided to the ED by the authorising officers by delegation containing the necessary information on	ICCU



Internal control principle	Model questions	Internal stake-holders
	the controls carried out, any weaknesses identified, and the actions taken to remedy these?	
Priority measure 3.4: Uses a combination of fraud control activities		
The Agency ensures that fraud control activities include a range, variety and mix of preventive and detective controls that also address the possibility of management overriding controls.		
10	3.4.1 (a) Has the Agency detected any leaks of sensitive information that have not followed the regulatory communication channels?	LSU/DPO/ ICCU/LISO
10	3.4.1 (b) If answer to Q. 3.4.1(a) is yes, did the Agency suffer any damages as a result of the leak?	LSU/DPO/ ICCU/LISO
10	3.4.1 (c) If answer to Q.3.4.1(b) is yes, have corrective actions been taken to identify the internal control weakness that have resulted in such leaks?	LSU/DPO/ ICCU/LISO
10	3.4.2 Are measures in place to prevent leaks of sensitive information?	LSU/DPO/ ICCU/LISO
10	3.4.3 Does the Agency perform a mapping of access to sensitive information? What can be improved?	LSU/DPO/ ICCU/LISO
10	3.4.4 Has the majority of staff involved in budget implementation and <i>ex post</i> controls received training on preventing and detecting fraud red flags fraud?	ICCU
10	3.4.5 Are rights and obligations, e.g., of economic operators, beneficiaries, experts, etc., defined in a clear and unambiguous manner?	PFMU/ ICCU
10	3.4.6 Does a list of fraud red flags for financial procedures (other than procurement and grants) exist and regularly updated?	FINU/ICCU
10	3.4.7 Is there a list of red flags for procurement fraud available and regularly updated?	PFMU/ ICCU
10	3.4.8 Is there a list of fraud red flags related to grants available and regularly updated?	PFMU/ ICCU
10	3.4.9 Does the Agency use open sources (e.g., internet searches) for basic checks of tenderers, grant applicants and experts having signed a declaration of absence of conflicts of interest?	PFMU/ ICCU
10	3.4.10 Is the Early Detection and Exclusion System (EDES) systematically consulted?	C1/C2/C3/ FINU/ PFMU/ AccO/ICCU
10	3.4.11 Are <i>ex post</i> controls, the IAS's and ECA's observations and recommendations taken seriously and implemented in a timely manner to help reduce the risk of irregularities? What can be improved?	ICCU



Internal control principle	Model questions	Internal stake-holders
10	3.4.12 Are adequate procedures in place to manage and approve at the appropriate management level exceptions and non-compliance events?	ICCU
10	3.4.13 Is a system in place to regularly monitor and review exceptions and non-compliance events that might indicate potential fraud red flags?	ICCU
10	3.4.14 Is there a procedure in place within the EUAA that allows the ED to notify the European Parliament, the Council, the ECA and the accounting officer of the Commission of any decisions/internal rules on financial matters (including those on delegations and nominations) within two weeks of their adoption?	FINU/ PFMU/ BSSU/ICCU
10	3.4.15 Are maximum limit amounts for authorisations (sub-)delegated based on a risk assessment endorsed by the ED to RAOs in accordance with the EUAA's organisational structure and defined in a homogenous manner and in proportion to the correspondent risk of the powers (sub-) delegated?	FINU/ICCU
10	3.4.16 Are ceilings for all budget regimes (e.g., Income (I), Hors (H) budget, etc.) and/or for all specific financial operations (e.g., payments, commitments, recovery orders, waiver of the recovery of amounts receivable, etc.) defined in the (sub-) delegation/nomination forms approved by the ED?	FINU/ICTU/ ICCU/AccO
11	3.4.17 Are the ABAC security rights related to the specific budget regimes and/or financial operations consistent with the nomination/(sub-)delegation decisions approved by the ED?	FINU/ICTU/ ICCU
11	3.4.18 Are financial and accounting central systems available at the EUAA properly managed by effectively ensuring security access rights for fraud prevention and detection? What can be improved?	FINU/ PFMU/ AccO/ICTU/ ICCU
10 & 11	3.4.19 Is an adequate contract management monitoring tool in place, duly documented and approved at the right level; and is such a tool being used effectively to monitor legal commitments and to avoid intentional spending beyond the maximum regulatory ceilings?	C1/C2/C3/ PFMU/ICTU /ICCU
11	3.4.20 How does the Agency maintain protection of the relevant IT systems?	ICTU/ICCU/ LISO
11	3.4.21 Are decisions to replace or further develop existing IT financial systems supported by a well-documented, cost-effective analytical approach and approved at the right level of management to prevent staff and potential contractors from colluding to develop/replace systems that do not meet business needs?	FINU/ICTU/ ICCU/SC



Internal control principle	Model questions	Internal stake-holders
11	3.4.22 Are adequate controls in place to ensure that all IT projects have a business case, business owner and an IT steering committee/ project board before and after implementation and that valuable resources are not intentionally used for purposes other than the business needs and objectives of the Agency and agreed by management?	BSSU/ICTU/ICCU
11	3.4.23 Has the Agency adopted a (project) portfolio that is regularly reviewed and endorsed by the management to ensure that all projects are driven by business needs and duplications are avoided?	BSSU/ICTU/ICCU
11	3.4.24 Is a procedure developed and implemented to control the acquisition, development, and maintenance of ICT systems/software in order to ensure that the confidentiality, integrity, and availability of the data to be processed are adequately secured and the defined protection requirements are met?	ICTU/ICCU
11	3.4.25 Are adequate information security controls in place for detecting, reporting, and responding to anomalous activities and threats, like physical or logical intrusion, breaches of confidentiality, integrity and availability of information assets, malicious code and publicly known vulnerabilities for software and hardware?	ICTU/ICCU/ LISO/BSSU
11	3.4.26 Are security awareness programmes periodically conducted to educate staff members on how to address IT information security related risks?	ICTU/ICCU
11	3.4.27 (a) Do the information security officers within the Agency perform their responsibilities independently from system and data owners?	ICTU/ICCU
11	3.4.27 (b) Are local information security officers within the Agency clearly aware that they can directly report to the highest level of management and/or to the appointing authority if their independence is impaired in the performance of their duties?	ICTU/ICCU
<p>Priority measure 3.5: Deploys control activities through policies and procedures</p> <p>The EUAA ensures that fraud control activities are well documented and implemented through policies and procedures.</p>		
10	3.5.1 Are the internal instructions on the use of Early Detection and Exclusion System (EDES) duly documented and approved at the adequate level?	FINU/ PFMU/ AccO/ICCU
12	3.5.2 Are the necessary control activities in place to reduce the risk of fraud/irregularity in sensitive functions to an acceptable level?	ICCU



Internal control principle	Model questions	Internal stake-holders
10	3.5.3 Are the required control activities in place to ensure that the Agency is compliant with the different national rules on temporary agency workers?	LSU/ICCU
10	3.5.4 Are the required control activities in place to ensure that the Agency is compliant with the principles of non-discrimination, equal treatment, and absence of conflicts of interest when selecting and contracting external experts?	PFMU/ICCU
10	3.5.5 Are adequate procedures and controls in place to make sure that the procurement file and all supporting documents are duly documented and filed, thus ensuring integrity, authenticity, reliability, timely access and a proper audit trail?	PFMU/ICCU
12	3.5.6 Is there specific guidance to assist operational units in preventing and detecting procurement and contract management fraud?	C1/C2/C3/ PFMU/ ICCU
12	3.5.7 Does the Agency have an <i>ex ante</i> risk-based internal control strategy that has been duly documented and approved at the right level of management, defining the <i>ex ante</i> controls on procurement and financial operations implemented by the Agency and documenting to what extent the applied <i>ex ante</i> control activities address the anti-fraud objective defined in Article 30 of the Agency's Financial Regulation?	FINU/ PFMU/ ICCU
12	3.5.8 Are the tasks and checks that need to be performed by the <i>ex ante</i> control functions for every step in each financial operation workflow in order to mitigate the risk of irregularity or fraud duly documented and agreed by the staff and approved at the adequate level?	C1/C2/C3/ FINU/ PFMU/ ICCU
12	3.5.9 Does the Agency have a defined control strategy in relation to grants?	PFMU/ BSSU/ICCU
<p>Fraud risk management objective 4: Fraud investigation and corrective action</p> <p>The EUAA establishes a communication process to obtain information about potential fraud and deploys a coordinated approach for investigation and corrective action to address fraud appropriately and in a timely manner.</p>		
<p>Priority measure 4.1: Establishes fraud investigation and response protocols</p> <p>The Agency establishes processes for communication relating to potential fraud.</p>		
14	4.1.1 Do internal guidelines clearly define reporting channels to be used and processes to be followed when staff comes across a suspicion of fraud?	ICCU
<p>Priority measure 4.2: Conducts investigations</p> <p>The Agency has in place the means to undertake investigations of potential fraud, giving due consideration to the scope, severity, credibility, and implications of communicated matter.</p>		
14	4.2.1 Does the Agency have the means to investigate potential fraud?	ICCU



Internal control principle	Model questions	Internal stake-holders
15	4.2.2 Is cooperation between the OLAF and the Agency well-developed and running smoothly?	LSU/ICCU/ OLAF correspondent
<p>Priority measure 4.3: Takes timely corrective action</p> <p>The Agency selects transparent corrective measures and particularly discipline, remediation, asset recovery, training, civil action and/or criminal referral to address in a timely manner the findings of the investigation.</p>		
15	4.3.1 Does the management demonstrate a high-level of transparency, commitment and clear intention to address the internal control deficiencies, irregularities and fraud red flags?	ICCU/SC
15	4.3.2 Does the Agency have in place a procedure and/or internal guidance that governs the conduct of disciplinary proceedings?	LSU/ICCU
<p>Fraud risk management objective 5: Fraud risk management monitoring activities</p> <p>The EUAA selects, develops, and performs ongoing evaluations to ascertain whether each of the five fraud risk management objectives are present and functioning and communicates the anti-fraud strategy action plan in a timely manner to parties responsible for taking corrective action, including the SM and MB.</p>		
<p>Priority measure 5.1: Considers a mix of ongoing and separate assessments</p> <p>The SM includes a combination of ongoing and annual monitoring processes to assess whether the fraud risk management objectives and priority measures were effectively achieved.</p>		
16	5.1.1 Is the Agency's coverage of financial <i>ex post</i> controls on financial operations and procurement procedures sufficient to reasonably mitigate the risk of fraud?	ICCU
16	5.1.2 Is the fraud risk register action plan monitored and re-assessed on a regular basis and made available to external and internal stakeholders?	ICCU
<p>Priority measure 5.2: Establishes appropriate measurement criteria</p> <p>The SM establishes appropriate measurement criteria to assist in the objective assessment of the anti-fraud strategy.</p>		
16	5.2.1 Did the Agency establish any internal control monitoring criteria (key performance indicators (KPIs)) to enable the objective assessment of the AFS?	ICCU
<p>Priority measure 5.3: Assesses, communicates and remediates deficiencies</p> <p>The SM assesses the results of the fraud risk management monitoring programme, communicates deficiencies to those tasked with corrective actions and ensures appropriate remediation is implemented promptly.</p>		
17	5.3.1 Does the Agency use standard contracts/agreements (for procurement etc.) containing anti-fraud clauses (suspension of payments/contracts, liquidated damages, etc.)? Is there	PFMU/ ICCU



Internal control principle	Model questions	Internal stake-holders
	guidance explaining under which circumstances these clauses can be applied?	
17	5.3.2 (b) Does the Agency use standard agreements for grants containing anti-fraud clauses? Is there guidance explaining under which circumstances these clauses can be applied?	PFMU/ ICCU
17	5.3.3 Where financial irregularities have been identified by control bodies and/or <i>ex post</i> controllers or fraud cases have been investigated by the OLAF, is there a clearly documented process explaining the roles and responsibilities to ensure the implementation of timely precautionary measures or recovery action (if applicable)?	C1/C2/C3/ FINU/LSU/ ICCU/AccO
17	5.3.4 Where financial irregularities have been identified by control bodies and/or <i>ex post</i> controllers or fraud cases have been investigated by the OLAF, is there a clear documented process explaining the roles and responsibilities to ensure the timely reporting of the financial irregularity to the Commission in line with the provisions of the Agency's Financial Regulation?	C1/C2/C3/ FINU/LSU/ ICCU
17	5.3.5 Is the MB kept updated on a regular basis on the outcome of the risk management process (including the fraud risk management process) and on the state of play of the resultant action plans?	ICCU/MB Secretariat
17	5.3.6 Are preliminary findings promptly shared, explained, and validated with RAOs when internal control weaknesses or financial irregularities are identified during <i>ex post</i> control?	ICCU/AccO
17	5.3.7 Are control arrangements in place to ensure accountability of those functions responsible for the timely implementation of fraud risk responses (control activities)?	ICCU
17	5.3.8 Is management aware of the repercussions for the Agency if corrective actions to rectify the internal control weaknesses identified by control bodies and/or <i>ex post</i> controllers are not implemented in a timely manner?	ICCU



Annex 4: Outline content headings of an anti-fraud strategy

1. Background
 - 1.1 General context
 - 1.2 The EUAA's context
2. Scope
3. Guiding principles of the EUAA's strategy
4. Definition of fraud for the purposes of the anti-fraud strategy
5. Main actors involved in addressing and preventing fraud
6. Fraud risk management objectives
7. Fraud risk assessment
8. Priority measures and control activities
9. Monitoring and reporting

Annex: Action plan



Annex 5: Fraud risk register action plan headings

The following headings are recommended for the fraud risk register action plan.

- Fraud risk management objective number;
- Fraud risk management objective;
- Priority measure;
- Risk title and description;
- Likelihood – of risk;
- Impact – of risk;
- Risk severity;
- Control objective;
- Risk responses (control activity) – to mitigate the identified fraud risks;
- Owner – entity(ies) responsible for the implementation of the risk response;
- Target date - of implementation of the risk response.

The following heading should be added when reporting on the status of implementation of the action plan.

- Implementation status (planned, in progress, implemented) - of the risk response.