

# MANAGEMENT BOARD DECISION

## DECISION No MB/2025/03

### OF THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

#### on the Anti-Fraud Strategy and its Action Plan for 2025-2027 (Recast of the MBD 2021/05)

#### THE MANAGEMENT BOARD OF ENISA

##### Having regard to

- The Treaty on the Functioning of the European Union (TFEU), in particular Article 325.1;
- The Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast);
- The Regulation (EU) (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), in particular Article 15.1 (h), 20.1 (k) and 33;
- The Staff Regulations of Officials, laid down by Council Regulation (EEC, EURATOM, ECSC) No 259/68 (hereinafter referred to as "Staff Regulations") and to the Conditions of Employment of Other Servants of the European Union (hereinafter referred to as "CEOS"), both as latest amended by Regulation (EU, EURATOM) No 1023/2013 of the European Parliament and of the Council of 22 October 2013, and in particular, Articles 11a, 12b, 16 and 22a;
- Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (Framework Financial Regulation (FFR));
- The Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee, the Committee of the Regions and the Court of Auditors on the Commission Anti-Fraud Strategy Action Plan - 2023 revision COM(2023) 405 final;

- The Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee, the Committee of the Regions and the Court of Auditors on the Commission Anti-Fraud Strategy: enhanced action to protect the EU budget (COM/2019/196 final);
- The Decision No MB/2024/10 of the Management Board of the European Union Agency for Cybersecurity (ENISA) on the establishment of ENISA's internal structures;
- The Decision No MB/2021/15 of the Management Board of the European Union Agency on rules for prevention and management of conflicts of interest and repealing Decision No MB/2013/7;
- The Decision No MB/2021/5 of the Management Board of the European Union Agency for Cybersecurity (ENISA) on Anti Fraud Strategy and its Action Plan;
- The Decision No MB/2019/13 of the Management Board of the European Union Agency for Cybersecurity (ENISA) delegating the relevant appointing authority powers to the Executive Director;
- The Decision No MB/2019/8 of the Management Board of ENISA the European Union Agency for Cybersecurity on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 of the European Parliament and of the Council (hereafter "ENISA's Financial Rules");
- The Decision No MB/2018/10 of the Management Board of the European Union Agency for Network and Information Security (ENISA) Guidelines on Whistleblowing;
- The Decision No MB 2013/16 of the Management Board of the European Union Agency for Cybersecurity (ENISA) concerning terms and conditions for internal investigations in relation to the prevention of fraud, corruption and any illegal activity detrimental to the Union's interests;
- The Decision No 02/2023 of the Executive Director of the European Union Agency for Cybersecurity (ENISA) on ENISA Code of conduct;
- The Decision No 86/2021 of the Executive Director of the European Union Agency for Cybersecurity (ENISA) on the Sensitive Functions at ENISA.

## Whereas

- ENISA, being an Agency governed by the European Union law, is bound to follow the financial rules set out in the Framework Financial Regulation (FFR) for the bodies referred to in Article 70 of the Financial Regulation (Regulation (EU, Euratom) 2024/2509).
- The European Union (EU) budget represents taxpayers' money to be spent only for implementing the policies approved by the EU legislator. Fraud involving EU funds has a particularly negative impact on the reputation of the EU institutions and on the implementation of EU policies.

- The Framework Financial Regulation (FFR) stipulates that the internal control system put in place should allow the prevention, detection, correction and follow-up of fraud and irregularities (Article 30(2)(d)) and the avoidance of conflict of interest (Article 30(3)(c) and Article 42).
- On 29 April 2019, the Commission adopted its revised Anti-Fraud Strategy. The action plan accompanying this document<sup>1</sup> tasked the European Anti-Fraud Office of the Commission (OLAF) with providing a methodology and guidance for Anti-Fraud Strategies (AFS) for EU agencies and other EU entities.
- OLAF has developed an updated Methodology and guidance for anti-fraud strategies for EU decentralised agencies (Ref. Ares(2024)4040978-05/06/2024).
- The European Commission also developed a Common Approach for the EU decentralised agencies that, among others, outlines principles for prevention, detection and investigation of fraud, corruption, irregularities and other illegal activities.<sup>2</sup>
- The ENISA Anti-Fraud Strategy and Action plan 2021-2024 was adopted by the Management Board Decision No MB/2021/05 and should be updated within 2024 as per the art 2 (1) of the MBD 2021/05 for the next reference period (2025-2027).
- As per the recommendation of the Methodology from OLAF, the Agency has carried out the evaluation of the Anti-Fraud Strategy 2021-2024 and prepared an Activity Report for the referenced period.
- The ENISA's Anti-Fraud Strategy should take into account the objectives set by the European Commission in its Anti-Fraud Strategy Action Plan, revised in 2023 (COM(2023) 405 final), which is based on lessons learnt, actions implemented and experience acquired in this field. This will allow ENISA to pro-actively continue to reinforce a strong anti-fraud culture and actively encourage fraud prevention with dedicated actions designed to the specifics of the ENISA activities.

## HAS DECIDED

### Article 1

To adopt the ENISA Anti-Fraud Strategy for the period of 2025- 2027 and its action plan annexed to this Decision.

### Article 2

(1) This Anti-Fraud Strategy enters into force on the day of its adoption and shall be reviewed in 2027 or earlier if deemed necessary.

---

<sup>1</sup> Revised in 2023, Commission Anti-Fraud Strategy Action Plan - 2023 revision (COM(2023) 405 final).

<sup>2</sup> [The Common Approach of the European Union adopted in July 2012 and its Roadmap](#), p. 66.



(2) The Action plan for the period of 2025-2027 and the Activity Report for the Anti-Fraud Strategy 2021-2024 are annexed to the present decision.

Done by written procedure on 10 February 2025.

For ENISA  
On behalf of the Management Board

[Signed]

Ms Fabienne Tegeler  
Chair of the Management Board





# ENISA ANTI-FRAUD STRATEGY

## 2025- 2027



# 1. GENERAL CONTEXT

The European Union (EU) budget represents taxpayers' money to be spent only for implementing the policies approved by the EU legislator. Fraud involving EU funds has a particularly negative impact on the reputation of EU institutions and on the implementation of EU policies. Articles 317 and 325 of the Treaty on the Functioning of the European Union (TFEU) are the legal basis regarding the protection of the financial interests of the Union and the fight against fraud affecting these interests.

On 29 April 2019, an updated Commission Anti-Fraud Strategy (CAFS) 2019 was adopted. After evaluating the 2011 CAFS, it was concluded that the strategy was still relevant and effective as a policy framework for the Commission protecting the EU budget. The action plan accompanying that Strategy tasked the European Anti-Fraud Office of the Commission (OLAF) with providing a methodology and guidance for Anti-Fraud Strategies (AFS) for EU agencies and other EU entities.

In 2023, the Commission has revised its Action Plan annexed to the CAFS, aiming to strengthen all parts of the anti-fraud cycle: prevention, detection, investigation and correction. The revised Action Plan complements a number of other policy initiatives, such as the proposal for an interinstitutional Ethics Body, the Anti-corruption package<sup>3</sup>, the recast of the Financial Regulation<sup>4</sup>, the Rule of Law mechanism<sup>5</sup> and the Conditionality mechanism<sup>6</sup>. It also complements the independent investigations conducted by the European Anti-Fraud Office (OLAF) and the European Public Prosecutor's Office (EPPO).

The European Commission has also developed a Common Approach<sup>7</sup> on EU decentralised agencies that requires a set of anti-fraud measures to be put in place by the agencies. Taking into consideration the priorities set by the European Commission within the framework of the Common Approach on EU decentralised agencies, the need to pursue the European Commission's main objectives for its implementation ("more balanced governance, improved efficiency and accountability and greater coherence"), the Management Board of ENISA adopted its Anti-Fraud Strategies and the related Action Plans in 2014 and 2021, which is now updated according to the future obligations and target points for the years 2025-2027.

Moreover, the Anti-Fraud Strategy and its action plan should be aligned with provisions of the Article 33 of the Regulation (EU) 2019/881. This provision calls upon ENISA to combat fraud, corruption and other unlawful activities. The Anti-Fraud Strategy is part of the legal framework of the Agency and meets the requirements of Article 32 of the Framework Financial Regulation of the European Commission which refers inter alia to the need to prevent and detect irregularities and fraud. The updated OLAF's Methodology and guidance for anti-fraud strategies for EU decentralised agencies point out that "the Anti-Fraud Strategy is part of risk management, but given the importance and complexity of the issue, fraud should be addressed in a dedicated

<sup>3</sup> [Proposal for a Directive of the EU Parliament and of the Council on combating corruption.](#)

<sup>4</sup> Adopted in 2024 as the [Regulation - EU, Euratom - 2024/2509 - EN - EUR-Lex.](#)

<sup>5</sup> [COM\(2019\) 163 final.](#) [COM\(2019\) 343 final.](#)

<sup>6</sup> [Regulation \(EU, Euratom\) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget.](#)

<sup>7</sup> [Joint statement on decentralised agencies.](#)

process, which runs on top of the annual risk management exercise, though closely interlinked with it". Therefore, although it is part of the internal control system, the ENISA Anti-Fraud Strategy must be considered as a separate, additional tool to further strengthen the internal control systems.

The ENISA Anti-Fraud Strategy 2025-2027 (the 'Strategy') is based on the ENISA Anti-Fraud Strategy 2021-2024, while it further consolidates and further develops the objectives set out previously. ENISA has implemented several tools to improve the prevention and detection of fraud. In particular, ENISA carries out an annual risk assessment exercise, taking into account the fraud risks at the Agency. The present strategy derives from this knowledge and aims at consolidating and further refining the anti-fraud activities at the Agency in a way which is proportionate to the fraud risks, having due regard to the costs and benefits of the measures to be implemented.

## 2. THE ENISA CONTEXT

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States and EU institutions, bodies and agencies (EUIBAs) on cybersecurity. It contributes to developing and implementing the Union's cybersecurity policies.

ENISA's aim is to strengthen trust in the connected economy, boost resilience and trust of the Union's infrastructure and services and keep our society and citizens digitally secure. It aspires to be an agile, environmentally and socially responsible organisation focused on people.

ENISA Single Programming Document for the years 2025 to 2027 sets out the activities that ENISA will undertake in the years 2025 to 2027 in accordance with the Agency's founding Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act) and takes into account the new ENISA Strategy <sup>8</sup>, the transposition of the NIS2 Directive, publication of the Cyber Resilience Act (CRA) and the expected publication of the Cyber Solidarity Act (CSoA).

The main stakeholders of the Agency are, i.a:

- The European Commission;
- EU Member States;
- The ENISA Advisory Group and National Liaison Officers Network;
- The Stakeholders Cybersecurity Certification Group.

Other major stakeholders include a number of Ad Hoc Working groups/expert groups established to contribute to the implementation of the ENISA Single Programming Document.

---

<sup>8</sup> [MB Decision 2024-14 on ENISA Strategy.](#)

The management of funds is not delegated to any member state and/or organization. All procurement procedures and calls are managed by ENISA.

ENISA implements its budget in accordance with the principles of sound financial management (Article 317 TFEU) and complies with the provision of Article 325 TFEU, according to which the EU and the Member States shall counter fraud and any other illegal activities affecting the financial interests of the Union. These articles provide an explicit legal basis for operations by the EU and its bodies and agencies to combat fraud and other unlawful activities. In this light, ENISA is committed to ensuring that the framework, the policies, the rules and the procedures in place enable the effective prevention and detection of fraud.

As of 2022, ENISA was entrusted a significant amount for the Support Action, which then found its way in 2024 in the Contribution Agreement between the European Commission (DG Communications Networks, Content and Technology) and ENISA to support member States with cybersecurity measures (ex post and ex ante). This significant increase of ENISA's budget also leads to the increase of the fraud risks that the Agency may be exposed to.

In addition to that, ENISA has been assigned to a growing number of tasks, i.a. stemming from the newly adopted EU legal acts (DORA Regulation, NIS2 Directive, Cyber Resilience Act, Cyber Solidarity Act).

ENISA staff, as of 31/12/2024, consists of 161 people, out of which 122 are statutory staff members (Temporary Agents and Contract Agents) and 39 are Seconded National Experts, interim agents, intra and extra muros.

Taking above into consideration and the limited human resources of ENISA so to duly fulfil its mandate, the Agency's exposure to risks, including those related to fraud, are higher in comparison with the recent update of the AFS performed in 2021.

## 3. DEFINITIONS<sup>9</sup>

### 3.1 FRAUD

Fraud is a deliberate act of deception intended for personal gain or to cause a loss to another party.

For the purposes of the Agency's Anti-Fraud Strategy, the term 'fraud' should be understood in a broad sense, encompassing:

- Fraud, corruption and misappropriation affecting the Union's financial interests, as defined in Articles 3 and 4 of the PIF Directive;
- 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

<sup>9</sup> Please refer to Annex II for detailed list of definitions relevant to this strategy.



defined in Article 1(2) of Regulation (EC, Euratom) No 2988/95 (insofar as they are intentional but not already captured by the criminal offences referred to above);

- Any other illegal activity affecting the financial interests of the EU;
- Serious breaches of professional obligations by staff or members of the Management Board of the Agency, as referred to in Article 1(4) of the OLAF Regulation, in the second subparagraph of Article 2(1) of Commission Decision (EC, ECSC, Euratom) No 352/1999 and in Article 16 of the Staff Regulations, the latter as regards obligations after leaving the service.

In principle, fraud requires two elements to occur simultaneously:

- Breach of a rule, and,
- Intention to gain undue advantage (whether financial or not and for oneself or others) from the breach of such rule.

Fraud may be committed by external stakeholders or partners, such as contractors, candidates, but may also be committed by ENISA staff.

Fraud can involve a reputational risk and, therefore, instances of fraud may be considered as critical risks even where the financial impact is low. It also covers misbehaviour that may or may not have a direct impact on the EU's financial interests, such as some cases of forgery (in CVs for example), money laundering, concealment or destruction of material facts, breaches of confidentiality, or breaches of IT systems. Conflicts of interests that have intentionally not been declared, favouritism and collusion also belong to the category of fraud.

Fraud covers a range of irregularities and illegal acts characterized by deception or misrepresentation, damaging interests of the EU.

In summary, fraud affects the Agency's financial interests and/or has a negative impact on the European Union as a whole and/or the Agency's reputation.

### **3.2 AN IRREGULARITY**

Fraud differs from 'irregularity', which is an act which does not comply with EU rules and which has a potentially negative impact on EU financial interests, but which may be the result of genuine errors committed both by beneficiaries claiming funds and by the authorities responsible for making payments. If an irregularity is committed deliberately, it is fraud.

## **4. FRAUD RISK ASSESSMENT**

In an environment where a risk management policy is well designed and implemented, the risks associated with fraud are different from other risks as they will typically have a low likelihood of occurrence (the estimated probability that the risk will materialise) considering the controls in place but a large impact if they do (potential consequence should the risk materialise).

Impact does not limit to the financial dimension but it also takes into account any damage to the reputation of the Agency.

The Agency deals with both direct public procurement and recruitment in-house.

Public procurement, the largest channel of EU public spending, is known to be one of the most significant areas of fraud risk, therefore attractive for fraudsters using corruption as a way of facilitating fraud.

In order to support cooperation between the EU and national governments, our Agency pools technical and specialist expertise from both the EU institutions and national authorities and the EU population in general.

It is crucial for the reputation of ENISA that its staff is selected according to high standards and set criteria. For this reason, favouritism in employment procedures and contracts or other types of fraud needs to be avoided: the selection and related contract shall be the result of the choice of the best candidates. Breaches of both public procurement and recruitment rules can be prevented, minimised and avoided if comprehensive action plans, measures and initiatives are put in place, followed up and updated regularly.

The initiatives to be taken to that end are meant to gradually improve the quality of procurement and recruitment procedures and strengthen the fight against fraud.

In 2024, ENISA conducted its annual Risk Assessment exercise in parallel with the risk assessment performed by the European Commission Internal Audit Service (held in September 2024) In this context, interviews have been conducted with every Head of Unit, Team Leader and selected Head of Sectors. The outcome served as a data source for the enterprise risk assessment of the Agency, including also risks related to fraud.

The Agency participated also in the annual peer review risk assessment led by the EU Agencies Network upon the request of European Commission DG Budget, taking the role of the cluster coordinator for agencies and joint undertakings under DG CNECT.

**Annex III** lists the key risks related to fraud that should be considered for the Agency. The risks have been identified based on the following data and guidelines:

- annual ENISA's risk assessment;
- the 2021-2024 Anti-Fraud Strategy;
- annual assessment of the Internal Control Framework, annual ex-post controls and audit reports of the Court of Auditors or other external auditors;
- OLAF methodology for the decentralised agencies and lessons learned via the EU agencies network.

Following the risks identification, their importance has been assessed using the methodology of

the risk assessment as described in the Agency's risk management framework<sup>10</sup>, which is based on the relevant European Commission's risk management framework. Both, likelihood and impact of the risks were taken into account so to calculate the inherent risk and, considering the mitigation measures that are already implemented at ENISA, the residual risk value has been measured. To each residual risk at least one action has been assigned to mitigate it further.

The identified risks are described in the Annex III - Action Plan along with the fraud risk assessment.

It is noted that the conflict of interest is a risk that has been identified across different categories, i.e. regarding not only contractors of the Agency, but also candidates during recruitment procedures, Selection Board members or members of ENISA statutory bodies or external experts.

Measures that may be taken to manage the risk of fraud are as follows:

- Preventive measures: These include segregation of duties, sensitive posts policy, annual risk assessment, ex ante controls, management supervision, regular meetings and monitoring tools (financial and non-financial), awareness raising actions on general conduct and other measures.
- Auditing measures: Various checks and verifications are performed to detect any related issues. These consist of regular audits by the European Court of Auditors and the Internal Audit Service, internal controls assessment, ex post controls, etc. In addition, there is an annual audit of the accounts.

## 5. OBJECTIVES AND ACTIONS

Based on the fraud risks identified above, ENISA concentrates its efforts on achieving the set of objectives listed below, according to the specific areas identified above and aiming at covering the fraud cycle: prevention, detection, investigation and correction/sanctioning. ENISA needs to set certain objectives to counter fraud at all levels – the level of the Governing Board, the ENISA Staff and external contractors and thus maintain the public trust in ENISA activities.

Whilst prevention remains one of the most important objectives of the present Anti-Fraud Strategy, it is deemed appropriate to focus efforts on detection, in particular by internal reporting of any possible case of fraud as well as proactive random verification in some areas.

In order to address the risks identified in the section above, the following strategic objectives are put forward.

---

<sup>10</sup> [ENISA Risk Management Framework](#).

## 5.1 OBJECTIVE 1: MAINTAIN A HIGH LEVEL OF ETHICS AND ANTI-FRAUD CULTURE IN THE AGENCY

The objective follows the need to continuously communicate the rules and the ethical values of the EU Public service to ENISA staff. Anti-fraud and ethical considerations should be a natural reflex for everyone working at the Agency, in particular those whose tasks involve managing or controlling EU funds. It is understood that fraud deterrence is facilitated by widespread common knowledge and awareness of relevant rules underlining any activity of ENISA. ENISA should gradually strengthen trainings and awareness raising on ethics and anti-fraud, so as the anti-fraud knowledge base.

- The compulsory training course on ethics, integrity, fraud prevention and detection should be organised for newcomers and as refresher for the rest of the staff (with obligatory attendance at least once every two years). A workshop on the ENISA's Code of conduct and ENISA's internal culture should be organised to promote the values of ethics and integrity amongst staff members.
- The Anti-Fraud coordination function, which falls under the competence of the ENISA's Internal Controls Team, is in force to help tailor advice to the different units of ENISA as well as individually to newcomers.
- The Anti-fraud knowledge base (intranet website) is maintained and regularly updated.

The objective here is to ensure that all Staff of the Agency complies and maintains the highest standards of professional ethics (specifically in relation to the prevention and detection of fraud). It is highly important to maintain a general ethical culture at ENISA. Fraud prevention needs to be accompanied by a culture of integrity and service to the common interest, with the aim to maintain a good reputation of ENISA and trust in the programmes it develops.

## 5.2 OBJECTIVE 2: COMPLIANCE AND TRANSPARENCY MEASURES IN PROCUREMENT

The objective is to ensure procurement procedures are compliant and transparent throughout all stages of each process — from planning a procurement to contract implementation - while highlighting risk areas. To perform its tasks, ENISA is legally bounded by relevant EU public procurement rules<sup>11</sup> and cooperates largely with tenderers, contractors, /beneficiaries, /candidates, external experts, etc. This is why, it remains crucial to set-up measures and controls designed to detect and investigate fraud, in addition to the preventive measures (mitigating controls) already in place.

This objective is of paramount importance, within the perspective of the other objectives mentioned.

- Policies and procedures for declaring, assessing and managing conflicts of interests in procurement procedures and remuneration of external experts should be adopted and implemented;

<sup>11</sup> [Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.](#)

- Regular monitoring of contracts by Procurement Team and Project Managers, so as the updated list of contractors is maintained in ENISA Procurement iNet site;
- Training for project managers and staff concerned in order to achieve a better understanding of finance responsibilities (specifically regarding supporting documents and requesting contractors the signed legal commitments before the closure of the year) and to reinforce control by financial actors shall be organised annually.

### **5.3 OBJECTIVE 3: COMPLIANCE AND TRANSPARENCY MEASURES IN RECRUITMENT AND HUMAN RESOURCES**

This objective is to ensure compliance and transparency of all recruitment procedures at every stage of the process – from selection to employment contract signature.

Favouritism in employment procedures and employment contracts needs to be avoided. It is also understood that the recruitment fraud can also occur when a member of staff or applicant makes false representation, wrongfully fails to disclose information or abuses a position of trust for personal gain. During the recruitment process, making false representations of themselves by applicants can be considered a criminal offence. While lying on an application form, CV, or presenting a fake certificate or diploma, but presenting this information as real, fraud is being committed and can be prosecuted. Conducting background screening highlights CV or application misrepresentations and protects business.

This objective is of paramount importance, in the light of the other objectives mentioned. Staff play a key role in implementing and fostering a 'zero tolerance' culture towards fraud and corruption.

- Policies and procedures for declaring, assessing and managing conflicts of interests in recruitment procedures shall be adopted and implemented;
- Training and guidance documentation for Selection Board members should be provided on the need basis, at least every two years;
- A rolling review system for the control and follow-up of declarations of outside activities shall be designed and put in place.

### **5.4 OBJECTIVE 4: COMPLIANCE AND TRANSPARENCY MEASURES IN ASSETS MANAGEMENT/INVENTORY**

The objective is to ensure that the Agency's assets are not being used in a fraudulent and inappropriate way. It aims at ensuring that a proper policy is applied and procedures are compliant and transparent through all stages – from recording to declassification.

- Declassification exercise is done by the Declassification Committee at least once per year. Declassification exercise in Heraklion should be done before the closure of the Local

Office<sup>12</sup>;

- Policy on assets management/inventory should be updated along with the appointment of the new Declassification Committee.

### **5.5 OBJECTIVE 5: SUSTAIN A SYSTEM FOR INTERNAL REPORTING OF SUSPECTED FRAUD OR IRREGULARITIES**

The objective is to sustain a system of appropriate tools, applications, reporting mechanisms and guidance and to make these available in order to address all the areas presenting potential risk. It should also take account all systems and tools in place for internal controls framework.

- Verification of the signatures of the Charter of task and responsibilities by AODs, AOSDs, FIAs, FVAs is performed along with the ABAC Financial Delegation Approval in ARES workflow and verification on the annual declaration of assurance of AOs is performed annually;
- Sensitive posts policy implementation is monitored every 2,5 years and risk assessment of all functions at ENISA is performed once every 5 years;
- Performance of the ex-post control/audits and ex-ante controls are performed annually by FIA/FVA.

### **5.6 OBJECTIVE 6: ADVANCE DIGITALISATION AND THE USE OF IT TOOLS TO FIGHT FRAUD**

The objective is to engage corporate IT solutions to make the fight against fraud more effective and efficient where applicable. The Agency will therefore continue to explore possibilities to increase digitalisation and interoperability. There is also a need to further strengthen and broaden the use of existing IT tools such as EDES and SUMMA to prevent, detect and investigate fraud.

- Access right management and access control exercises are performed at least every 2 years.;
- An advanced [AI-based] IT tool to check plagiarism in grant-related documents should be acquired.

## **6. ROLES AND RESPONSIBILITIES**

While it is essential that all ENISA staff members should have a clear understanding of ENISA's Anti-Fraud Strategy and its action plan, some individuals and ENISA structural entities may have intrinsic roles or responsibilities and these are identified below.

---

<sup>12</sup> Planned to be closed by 30 June 2026 as per the [MB Decision 2024-06 on ENISA office in Heraklion](#).

## 6.1 ENISA MANAGEMENT BOARD

The Management Board of ENISA is responsible for the adoption of the ENISA Anti-Fraud Strategy which shall be proportionate to the fraud risks, having regard to a cost-benefit analysis of the measures to be implemented. Information on ENISA AFS implementation shall be part of ENISA Authorising Officer's Consolidated Annual Activity Report, as per Article 48 of ENISA Financial Rules.

## 6.2 ENISA EXECUTIVE DIRECTOR

The Executive Director of ENISA leads by example by promoting an anti-fraud culture across ENISA, sets anti-fraud objectives, monitors the implementation of the strategy and its action plan and puts in place effective arrangements for combating fraud.

The Executive Director will report once a year to the Chairman of the ENISA's Management Board on the ongoing or closed OLAF cases via the Annual Activity Report. Cases with significant financial or reputational risk are in addition reported during the closed sessions of the Meetings of the Management Board.

## 6.3 AUTHORISING OFFICERS BY DELEGATION (AOD)

The AOD is the "first line controls" for the prevention and detection of fraud. He/she is responsible for promoting the anti-fraud culture within their units/teams empowered to ensure staff awareness and facilitate the immediate reporting of suspected cases of potential fraud to the ENISA Executive Director/Internal Controls Team therefore without delay, and coordinating with all other actors involved in or responsible for the implementation of the Anti-Fraud Strategy.

Based on all the information at his disposal, the AOD has to decide on any actions to be undertaken which are determined by the specific circumstances of the case. The recovery action (or any other implementing investigation activity) falls under the responsibility of the AOD who may have recourse to several sources of information (such as audit reports, information received from the beneficiary after the end of the OLAF investigation), one of which is the OLAF final report.<sup>13</sup>

## 6.4 COMPLIANCE SECTOR/INTERNAL CONTROLS TEAM

The ENISA's Compliance Sector (Internal Controls Team) is responsible for identifying and advising regarding the risks of breach of legal provisions and breach of ethical behaviour rules which may lead to liabilities or reputational damage for ENISA. This includes to:

- coordinate the implementation of the Anti-Fraud Strategy (anti-fraud coordinator function);
- follow up on actions;
- report to the Executive Director on such implementations;
- act as a contact point for OLAF on strategy related issues and any trainings/info sessions, legal developments etc.;

<sup>13</sup> [Annex 3 Guidelines on use of OLAF Final Report.](#)



- provide advice, guidance on managing the fraud risk;
- propose additional controls;
- provide induction to the newly recruited staff.

## 6.5 INTERNAL CONTROL COORDINATOR

The Internal Control Coordinator coordinates the overall implementation of the agreed actions of the annual risk assessment, which include actions related to the Anti-Fraud Strategy. He/she is responsible to inform the Executive Director, whenever he/she identifies as part of the risk assessment or internal controls assessment any information relating to possible cases of fraud, corruption or other irregularities that could affect the Communities' financial interests.

## 6.6 STAFF MEMBERS

Staff members are subject to certain obligations laid down in the Staff Regulations (such as conflicts of interest, gifts, external activities, spouse's employment, or publications or speeches on EU-related matters (Articles 11, 11a, 12, 12b, 13, 15, 16, 17, 17a and 19 of the Staff Regulations)). They are obliged to report facts pointing to a possible illegal activity, including fraud or corruption, or to a serious failure to comply with the professional obligations as staff pursuant to Article 22a of the Staff Regulations.

All staff members are meant to comply with the ENISA Anti-Fraud principles and the present strategy. Staff are also expected to forward any reasonable concerns with regard to fraud to their Head of Unit, the Reporting Officer, and/or the Executive Director in accordance with the existing guidelines, for example, following the internal whistleblowing procedure.

## 7. ACTION PLAN

An action plan is created to meet the objectives mentioned above. This action plan is intended to implement the ENISA Anti-Fraud Strategy and ensure the sound management of public procurement, recruitment and the other risk areas identified. The ENISA Anti-Fraud Action Plan for the period of 2025 - 2027 is presented in the Annex III.

## 8. THE FRAUD REPORTING PROCEDURES

### 8.1 MECHANISM FOR REPORTING IRREGULARITIES OR ALLEGED FRAUD

All ENISA staff members (including seconded national experts, interim agents, or other external workforce working at ENISA) are expected to report irregularities and alleged frauds. Different mechanisms are in place to report possible fraudulent behaviour.

As per Article 22a of the Staff Regulations, staff members can report to their immediate supervisor or to the Executive Director. In case the staff member considers that taking such action might endanger their position, he or she can report directly to the Chair of the Management Board or to OLAF.



As per Article 22b of the Staff Regulations, staff members can alternatively address their concerns to another institution (e.g. President of the Commission or of the Court of Auditors or of the Council or of the European Parliament, or to the European Ombudsman).

As per Article 22c of the Staff Regulations, each institution shall in accordance with articles 24 and 90 of the Staff Regulations, put in place a procedure for the handling of complaints made by staff members concerning the way in which they were treated after or as a consequence of fulfilling their obligations under the above Articles 22a or 22b of the Staff Regulations.

Protection of whistleblowers is provided for in the ENISA whistleblowing strategy, which addresses also specifically the protection of personal data.

### 8.1.1 OPTION TO REPORT DIRECTLY TO ENISA

Staff members can report on alleged fraud directly, through the reporting template in Annex I of this Strategy (to be filled in and sent by email to the Executive Director or to the Chair of ENISA Management Board – available in word file: [Compliance - Template to report fraud - All Documents](#)).

### 8.1.2 WHEN TO REPORT TO OLAF?

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

Reporting on alleged fraud or serious irregularity can be done:

- In case the staff member who wishes to report considers that taking such action might endanger their position at the Agency;
- In case of alleged fraud or other serious irregularities with a potential negative impact for EU public funds, whether EU revenue, expenditure or assets held by EU institutions;
- In case of serious misconduct by members or staff of EU Institutions and bodies.

Fraud and irregularities are not to be confused with alleged maladministration or broader systemic issues by EU institutions and bodies. Such issues fall into the authority of the European Ombudsman as provided for in Article 22b of the Staff Regulations.

In case of suspicion of fraud, OLAF can be informed by Note to the Attention of its Director – General, which is registered in ARES,<sup>14</sup> by email with a SECEM protection to be used, or by postal mail. In addition, any informant can report suspected cases of fraud and corruption to OLAF, by using its [Fraud Notification System](#).

<sup>14</sup> [Contact OLAF, Reporting fraud & Fraud Prevention](#).

## 9. MONITORING, REPORTING AND COMMUNICATION OF THE AFS AND ITS RESULTS

The ENISA Compliance Sector (Internal Controls Team) shall ensure that ENISA manages the risk of fraud up-to-date with developments in best practice and legislative requirements and aligned with the OLAF methodology. The Anti-Fraud Strategy and its Action Plan shall be reviewed every three years.

ENISA AFS Action plan is subject to regular (at least quarterly) monitoring in conjunction with the Agency central risk register. Its implementation shall be included in the Single Monitoring Table maintained by the ENISA Compliance Sector and reported to the Management Team accordingly, no less than once per year.

It is also taken into account during the annual assessment of ENISA Internal control Framework, as the indicators are directly linked to the fraud risks identified and actions proposed in the Action Plan.

In addition, the internal dissemination and communication on the ENISA AFS is ensured by:

- uploading the present Management Decision on ENISA iNet and external website;
- news on iNet encouraging staff to follow dedicated training on fraud prevention, ethics and integrity and respect of dignity;
- regularly updating the status of the Fraud Risk Register and Action Plan on the Agency's iNet.

Such measures, together with others defined in the Action Plan, aim to raise staff and stakeholder awareness and continue developing an anti-fraud culture within the Agency.



## ANNEX I – REPORTING TEMPLATE FOR TRANSMISSION OF ALLEGED FRAUD

1. Please describe briefly the situation you wish to report.

2. How do the irregularities, fraud or corruption you want to report relate to the European Union?

3. Select the one or more options of the checkboxes below, as appropriate:

- Irregularities detrimental to ENISA Budget
- Serious misconduct by Members, Stakeholders or Staff of ENISA
- Serious violations of professional duties committed by ENISA's Staff
- I do not know

4. Please describe the facts as objectively as possible and explain how you have become aware of them. Please try to be accurate in your statement and, if possible, include verifiable information.

5. Please indicate the timeframe where the events being reported has occurred.

6. Have you reported those events to other bodies or authorities? If yes, please indicate the name(s) of these organisation(s) and the date you contacted them.



## ANNEX II – LEXICON

Non-exhaustive list of actions considered to fall within the definition of fraud or linked to fraud:

- **breach of confidentiality:** a situation when data or private information is disclosed to a third party without the data owner's consent. It is generally considered as a disclosure of confidential information (depending upon the definition of confidential information);
- **embezzlement:** it is the act of withholding assets for the purpose of conversion (theft) of such assets, by one or more persons to whom the assets were entrusted, either to be held or to be used for specific purposes. Embezzlement is a type of financial fraud;
- **conflicts of interests:** a situation where the impartial and objective exercise of the functions of a financial actor or other person is compromised for reasons involving family, emotional life, political or national affinity, economic interest or any other shared interest with a recipient;
- **collusion:** an agreement between two or more parties, sometimes illegal and therefore secretive, to limit open competition by deceiving, misleading, or defrauding others;
- **corruption:** an abuse of entrusted power for private gain. Corruption practices hurt everyone dependent on the integrity of people in a position of authority;
- **double claiming of costs:** submitting the same items of expenditure to different funding sources in parallel in order to obtain the same financial support from different parties;
- **extortion, blackmail, bribery:** requesting or accepting money or valuables to influence the award of a grant or contract;
- **falsification of documents:** it is the act of intentionally changing or modifying information on a document with the intention of misleading a person or company;
- **favouritism:** a preference given to acquaintances, friends and family over strangers. When public (and private sector) officials demonstrate favouritism to unfairly distributed positions and resources, they are guilty of cronyism or nepotism, depending on their relationship with the person who benefits;
- **fraudulent bankruptcy** may occur in various ways but one of the most common methods of indulging in fraud is to make false statements with regards to one's assets while filing a claim for bankruptcy protection. Concealment of assets from the court can be done by illegal transfer of money to family members or friends, shift the property or assets to offshore accounts and failing to report the various sources of income;
- **leakage of information** takes place when confidential information is revealed to unauthorized persons or parties;
- **non-compliance** with the provisions and/or legal requirements of the contract or grant agreement (e.g. non respect of the obligation to organize tenders or market consultations for subcontracted activities);
- **overcharging** (by forgery or alteration of documents, e.g. by knowingly generating false time sheets or invoices, by declaring fictitious contractors or employees or unjustified trips, or by using substandard materials);
- **plagiarism:** use or close imitation of the language and ideas of another author and representation of them as one's own original work;
- **wilful destruction** or removal of records intentionally.

## ANNEX III

# AFS ACTION PLAN FOR THE YEARS 2025-2027

EXCEL FILE

## ANNEX IV

ACTIVITY REPORT ON THE ANTI-FRAUD STRATEGY 2021-2024



No	Risk	Impact (1 to 5)	Likelihood (1 to 5)	Inherent risk	Mitigating measures in place	Residual risk (considering mitigation measures already in place)	Risk response	Action	Actors responsible	Indicator			Deadline	Link with the ICF indicator
										Description	Target value	Measured value after the action is completed		
<b>Anti-Fraud Objective 1 : Maintain a high level of ethics and anti-fraud culture in the Agency .</b>														
1	Insufficient training/awareness related to red flags of fraud that could result to fraudulent activities such as falsification of documents , inflated invoices etc. going undetected . This may	4	2	8	1.1. Organisation of training sessions dedicated to anti-fraud and ethics in the induction programme for newcomers so as refreshing sessions for staff, with the possible support of OLAF.	5 (low)	Accept	1.1. To organise training sessions dedicated to anti-fraud and ethics in the induction programme for newcomers so as refreshing sessions for staff, with the possible support of OLAF.	CSS HR (ethics and integrity), EDO (antifraud)	Percentage of newcomers undergoing the training, Percentage of staff undertaking refresher within 2 years [1]	100% (newcomers), 70%(refresher)		Annually	31,32

further result in loss of EU funds or unjustified/irregular payments.					1.2. Organisation of a workshop on the ENISA's code of conduct and ENISA's internal culture to promote the values of ethics and integrity amongst staff members.	1.2. To organise a workshop on the ENISA's code of conduct and ENISA's internal culture to promote the values of ethics and integrity amongst staff members.	EDO	Percentage of staff having completed the training.	70%		Every two years	4
					1.3. ABAC training for staff using the tool - FIA, FVA, AODs.	1.3. ABAC training for staff using the tool - FIA, FVA, AODs.	CSS (training)	Percentage of staff having access to ABAC completed the training.	70%	Annually	No indicator, 42 for four eyes principle	
					1.4. Maintaining and update of the online page with a template (Annex I) on ENISA's iNet for reporting on whistleblowing and fraud and fraud register for reported	1.4. Maintain and update an online page with a template (Annex I) on ENISA's iNet for reporting on whistleblowing and fraud and fraud register for	EDO	Number of cases of potential fraud and misconduct signalled by staff to the agency	<1	Continuously	31, 60	
						Number of cases of potential fraud and serious misconduct		0				



					fraud and irregularities. Maintain a dedicated page on the ENISA staff intranet for anti-fraud tools.			reported fraud and irregularities . Maintain a dedicated page on the ENISA staff intranet for anti-fraud tools.		t sent to OLAF for investigation.				
<b>Anti-Fraud Objective 2 :Compliance and transparency measures in Procurement.</b>														
<b>2</b>	Alleged favoritism of an external service provider and conflict of interest with this service provider by ENISA staff member which may indicate a collusion.	<b>4</b>	<b>2</b>	<b>8</b>	2.1. CEI list of experts, Declaration for Col forms in contracts with remunerated experts and procurement procedures.	<b>6 (medium)</b>	Reduce	2.1. Set-up of (new) detailed policies and procedures for declaring, assessing and managing conflicts of interests in procurement procedures and remuneration of external experts.	EDO and CSS/Procurement	Policies refined and adopted	Yes		Q2 of 2025	No indicator
										Sample monitoring of conflict of interest/assessment exercises	<5 erroneous/missing declarations		Annually	No indicator
<b>3</b>	Uncompleted/missing supporting documents	<b>3</b>	<b>1</b>	<b>3</b>	3.1. Ex-ante verification, four-eyes principle	<b>3 (low)</b>	Accept	3.1. Ex-ante verification, four-eyes principle	CSS					

<p>provided by Project Manager (in particular to obtain from contractors /suppliers complete supporting documentation including pro-forma invoices) and not verified carefully by FAP that may lead to erroneous process and further, to unlawful usage of EU funds.</p>				<p>3.2.Training for project managers and staff concerned in order to achieve a better understanding of finance responsibilities (specifically regarding supporting documents and requesting contractors the signed legal commitments before the closure of the year) and to reinforce control by financial actors.</p>			<p>3.1.Training for project managers and staff concerned in order to achieve a better understanding of finance responsibilities (specifically regarding supporting documents and requesting contractors the signed legal commitments before the closure of the year) and to reinforce control by financial actors.</p>		<p>Percentage of PMs and staff concerned completed the training.</p>	<p>100%</p>		<p>Annually</p>	<p>No indicator</p>
--	--	--	--	--	--	--	--	--	--	-------------	--	-----------------	---------------------

4	Irregular expenditure, such as improper use of allowances or inflated costs by a contractor for services provided to the Agency in the framework service contract that may lead to damage to ENISA budget.	3	1	3	4.1.Regular monitoring of execution of contracts, updated list of contractors published on Procurement iNet site.	3(low)	Accept	4.1.Regular monitoring of contracts via notification function of iNet, updated list of contractors published on Procurement iNet site.	EDO and CSS/Procurement	Percentage of exceptions with high risk registered.	0	Continuously	53
					Linked with actions 3.1. and 10.2.			Linked with actions 3.1. and 10.2.		Number of administrative and monetary incorrect transactions identified during ex-post control.	Minimum 5% for both in value and volume		Annually
<b>Anti-Fraud Objective 3 : Compliance and transparency measures in Recruitment and Human Resources</b>													
5	Risk for ENISA statutory bodies members and former staff to be involved in a specific “revolving	4	3	12	5.1. Set of policies and procedures for declaring, assessing and managing conflicts of interests for members of	10 (medium)	Reduce	5.1. Monitoring and managing of conflict of interests.	EDO	Policies defined and adopted	Yes	Q2 2025	4
					Number of signed declarations of absence of COI by MB, EB, AG and			90%		Quarterly	No indicator		

	doors” conflict of interest situation. If, f.ex., post-employment activity requests are not appropriately checked, it may lead to the inappropriate use of confidential information obtained during their prior employment at the Agency.				statutory bodies.				NLO members					
									Sample monitoring of conflict of interest/assessment exercises	<5% verified erroneous/missing declarations		Continuously	No indicator	
6	Breach of the duty of discretion and confidentiality of Selection Board members during the selection procedure.	4	3	12	6.1. Guidance provided to Selection Board members, Col forms, HR checks	10 (medium)	Reduce	6.1. Dedicated training and guidance document for Selection Board members.	CSS HR	Guidance developed	Yes		Q3 2025	No indicator
										Percentage of Selection Board members undergoing training (obligatory)	90%		On the need basis, at least every	No indicator

	Agency's exposure to the issue of conflict of interest can constitute a reputational risk to ENISA.												two years	
7	If outside activity requests are not checked in due time or appropriately, some of ENISA staff may engage themselves in the activity incompatible with the interests of the Agency.	3	2	6	7.1. Form to declare and outside activity and approval process by HoEDO.	5 (low)	Reduce	7.1. Design a rolling review system for the control and follow-up of declarations of outside activities.	EDO and CSS HR	Sample monitoring and verification	<5% non-declared activities		Annually + verification done on the case-by-case basis	No indicator
<b>Anti-Fraud Objective 4 : Compliance and transparency measures in Assets management/Inventory.</b>														
8	Misappropriation of assets; Use for private	2	2	4	8.1. Declassification exercise by Declassification Committee.	4 (low)	Reduce	8.1. Declassification exercise in Heraklion before	CSS/Declassification Committee	Report of the Declassification Committee	Yes		By mid 2026	No indicator

	needs; Undue declassification and donation of assets; Inadequate follow-up for updating purposes that may lead to in a loss of EU funds.							closure of local Office.		e after the exercise performed				
					8.2. Policy on assets management/inventory.			8.3. Update of the policy on assets management/inventory. Appointment of the new Declassification Committee to be done by the means of the EDD.					By Q3 2025	No indicator
<b>Anti-Fraud Objective 5: Maintain a functional system for internal reporting of suspected fraud or irregularities.</b>														
9	Abuse of decision making capacity, binding agency by signature (AO, AOD, AIPN), approvals or capacity to influence decisions	4	1	4	9.1. Verification of the signatures of the Charter of task and responsibilities by AODs, AOSDs, FIAs, FVAs. Verification on the annual declaration of assurance of AOs.	4 (low)	Accept	9.1. Verification of the signatures of the Charter of task and responsibilities by AODs, AOSDs, FIAs, FVAs. Verification on the annual declaration	EDO	Percentage of the signed declarations of assurances and charter of tasks and responsibilities.	100%		Annually	8, 9

	(capacity to collect, present and link, factual elements that support any decision making process).							of assurance of AOs.						
					9.2. Monitoring of the sensitive posts policy implementation. A risk assessment of all functions at ENISA performed once every 5 years.			9.2. Monitoring of the sensitive posts policy implementation. Next risk assessment to be performed in 2026.	EDO	Report to the Management Team at least once every 2,5 years on the measures applied.	Yes/No with justification		Every 2,5 years - monitoring, every 5 years - risk assessment	44
10	There may be a failure in the implementation of the internal controls system, causing f.ex. management of overriding financial controls.	2	3	6	10.1. EDD on financial circuit/ Ex-ante financial verification.	4 (low)	Reduce	10.1. Revision of the EDD on financial circuit and update of single monitoring table. Ex-ante financial verification.	EDO	Four eyes principle has been ensured in all financial and non-financial workflows (design of financial circuits and operational workflows)	Yes/No with justification		For EDD revision - Q1 of 2025, for the single monitoring table - twice per year	42, 64

					10.2. Performance of the ex-post control/audits and ex-ante controls by FIA/FVA.			10.2. Performance of the ex-post control/audits and ex-ante controls by FIA/FVA.	EDO	Percentage of ex-ante financial verification and ex-post control financial transactions	Minimum 5% for both in value and volume		Annually	37, 38
<b>Anti-Fraud Objective 6: Advance digitalisation and the use of IT tools to fight fraud.</b>														
11	Leak of sensitive information/willful disclosure which may, i.a. damage the Agency's reputation.	3	3	9	11.1 Access control/security measures in place.	6 (medium)	Reduce	11.1 To perform access right management and access control exercises.	CSS IT/ISO/AB AC neutral verifier	Number of identified improper access granted during the control.	<5		Annually	41 - for ABAC access rights, 58
12	Plagiarism due to the incomplete verifications with appropriate IT tools and with relevant EU institutions, bodies, offices or agencies which may damage the	2	2	4	12.1 Untiplagiarism tool in place	4 (low)	Reduce	12.1 To acquire an advanced [AI-based] IT tool to check plagiarism in grant-related documents and raise awareness among staff on its usage.	EDO/Communication sector/IPR MC	Number of potential cases of plagiarism detected by the agency's IT tool for plagiarism detection	<5		2025	No indicator







## ANNEX IV TO THE MBD 2025-03 ON THE ANTI-FRAUD STRATEGY AND ITS ACTION PLAN FOR 2025-2027 (RECAST OF THE MBD 2021/05)

# ACTIVITY REPORT ON THE ANTI-FRAUD STRATEGY 2021-2024

## 1. INTRODUCTION

By the means of the Decision No MB /2021/5<sup>1</sup> of the Management Board of the European Union for Cybersecurity, ENISA adopted its Anti-Fraud Strategy and the Action Plan for the years 2021-2024. As provided for in this Decision, it shall be reviewed in 2024 and the Activity report on the activities implemented to achieve its goals shall be created by 1/07/2024.

In this regard, the present report is aimed to assess the actions taken by the Agency during the last 3 years to meet the objectives of the Anti-Fraud Strategy.

This assessment is also important so to set up new objectives for the next 3-years strategy, with a view on the Agency structural adjustment as from the 2025 and the new assignments and occupation of the sensitive posts.

## 2. STRATEGIC OBJECTIVES ACHIEVEMENTS

### 2.1 OBJECTIVE 1 - INTEGRITY AND COMPLIANCE THROUGH EFFICIENT AND TARGETED COMMUNICATION ON ETHICS AND FRAUD AWARENESS

In order to enhance the communication on ethics and fraud awareness, the Agency has undertaken several actions.

1. A dedicated webpage on iNet: [Anti-Fraud - Home](#) has been created so to inform ENISA staff about rules governing the detection, sanctioning and prevention of fraud within the Agency. It includes the following sections:
  - a) Legal and Policy Framework
  - b) Anti-Fraud Tool Box
  - c) Prevention-Detection-Sanction and recovery Investigation
  - d) Fraud Prevention and Detection Network (FPDNET)

---

<sup>1</sup> [05 2021 MB Decision 2021-5 on Anti-Fraud strategy.pdf](#)



- e) IDOC (Investigation and Disciplinary Office of the Commission)
- f) Trainings, including the information on the implementation of whistleblowing policy and procedures.<sup>2</sup>
- g) OLAF reports
- h) Reporting fraud and fraud prevention.

2. The Agency offered dedicated trainings, including ones delivered by OLAF expert. Additional session customised for managers has also been organised in 2023. A summary of trainings and participation rate is provided in the table 1.

Training material can be found in the section: [Trainings](#) of the [Anti-Fraud - Home](#) page.

Trainings covered the following topics:

- the potential risks in ENISA
- explaining the Fraud response plan (anti-fraud cycle/prevention/detection/reporting)
- presenting the procedure of an OLAF investigation
- presenting the Commission Anti-Fraud Strategy and its objectives
- explaining the notion of irregularity within the anti-fraud context
- explaining the notion of fraud and its scope
- explaining the ethical principles common to all staff members
- explaining the notion of conflict of interest and corruption
- explaining the notion of whistleblowing

**TABLE 1.**

Course name	Date	Number of Participants
Fraud awareness	15/09/2021	9
Fraud awareness	25/11/2021	5
Fraud awareness	23/06/2022	7
Fraud awareness	17/11/2022	6
Anti-fraud for managers	02/10/2023	19
Anti-fraud for all staff	03/10/2023	23
Fraud awareness	07/12/2023	19
Code of Conduct & anti-fraud	16/01/2024	19
Fraud awareness	29/05/2024	15
Fraud awareness Refresher	27/11/2024	10

3. The Agency has developed a comprehensive Code of conduct, outlining ENISA’s expectations regarding staff members’ behaviour and conduct towards their colleagues, supervisors and overall organization, so as towards citizens and stakeholders. It has been adopted by means of the ED Decision: [2023-02 ED Decision on the ENISA Code of Conduct](#).

Before its adoption, a dedicated Q&A session has been delivered by the Legal Adviser of the Agency, on the 27<sup>th</sup> September 2021. Another presentation on the adopted code of conduct was delivered during the strategy week on 16<sup>th</sup> January 2024.

Further to the presentations/trainings, the Anti-fraud coordinator/Legal Adviser has received a number of requests by staff members, especially on declaration of outside activities, declaration of gifts, as well as participation in conferences.

<sup>2</sup> [Reporting fraud & Fraud Prevention](#)



#### 4. Appointment of the Anti-Fraud Coordinator:

An Anti-Fraud Coordinator function has been established at ENISA. The Anti-Fraud Strategy defines the Anti-Fraud Coordinator as the person being „*responsible for identifying and preventing the risks of breach of legal provisions and breach of ethical behaviour rules which may lead to liabilities or reputational damage for ENISA*“.

ENISA Legal Adviser has been appointed to the Anti-Fraud Coordinator function for the period 2021-2024. As of 2025 the function shall be under the responsibility of the Compliance Sector/Internal Controls Team.

## 2.2 OBJECTIVE 2: COMPLIANCE AND TRANSPARENCY MEASURES IN PROCUREMENT

To meet this objective, ENISA has undertaken the following measures:

1. Procurement Team consult the EDES (Early-Detection and Exclusion System) to reinforce the protection of the Union's financial interests and to ensure sound financial management. On many occasions Procurement Team checks the eCertis website: <https://ec.europa.eu/tools/ecertis/#/search> to ensure that the tenderer is providing the legally correct type of form for the various evidences required to be obtained from their relevant State authorities.
2. In order to ensure legal compliance, the Legal Adviser is included in all procurement workflows related to the standardised Memorandum of Understandings. A number of cases were successfully resolved in close collaboration between the Agency's Procurement team and the Legal Adviser (e.g., notion of professional conflict of interest, review of legal documents of tenderers: detection of wrong power of attorney etc).
3. Further to the relevant ECA observations for the year 2021 on the absence of evaluation reports and award decisions for low-value contracts, they are now included in ARES (formerly-paperless) workflows.
4. The Agency has implemented the mandatory signing of declarations of conflict of interest and confidentiality declarations by all experts applying to a Call of Expression of Interest (CEI) list and by parties contracted through a procurement procedure.

## 2.3 OBJECTIVE 3: COMPLIANCE AND TRANSPARENCY MEASURES IN RECRUITMENT

In order to ensure the compliance and transparency of the recruitment procedures, the Agency has undertaken the following measures:

1. Revision of the templates of the ENISA vacancy notices have been performed. In this context, the possibility of the candidate to have his/her application reassessed by the Selection Board was especially clarified.

More precisely, candidates who feel that an error has been made in relation to their non-admission to the selection procedure (i.e., not eligible) or to their exclusion from the selection procedure (i.e., not invited for an interview/written test) may request a review within 10 calendar days from the date on which they are notified about the decision. Requests for internal review may be based on one or more of the following reasons:

- a. material irregularity in the competition process.
- b. non-compliance, by the Selection Board or ENISA, with the Staff Regulations and relevant implementing rules, the vacancy notice, its annex and/or case-law.

2. Each member of the Selection Board' (including observers) signs a declaration with regard to confidentiality. The Selection Boards' work and deliberations are bound by the principle of confidentiality as per Article 6 of Annex III of Staff Regulations. The name of the Selection Board members (and/or observers if applicable) are published on the ENISA website once established. It is strictly forbidden for the candidates to make any contact with the Selection Board, either directly or indirectly. Any infringement to this rule will disqualify the candidate from the competition.<sup>3</sup>
3. The template of the declaration of interest for the candidates for taking part in the recruitment procedures is available on iNet. It aims to assess whether a potential or actual conflict of interest exists which could impair the impartiality and the independence of the candidate regarding his/her future responsibilities in relation to the specific position on-offer and to identify the appropriate measures to be adopted by the Executive Director, if any.<sup>4</sup>

## 2.4 OBJECTIVE 4: COMPLIANCE AND TRANSPARENCY MEASURES IN ASSETS MANAGEMENT/INVENTORY

To meet this objective, the Agency has in force a Policy on Inventory Management, adopted by the [2013-74 EDD On Inventory Management](#). It has been amended by the [EDD 2022-29 amending the ED Decision No 74/2013](#) which established a new declassification committee for the period of two years (mandate until 07/07/2024).

During the period of 2021-2024, the Declassification Committee has performed its exercise and presented the report to the Executive Director to issue the respective decision on the declassification of inventory items.

## 2.5 OBJECTIVE 5: ESTABLISH A SYSTEM FOR INTERNAL REPORTING OF SUSPECTED FRAUD OR IRREGULARITIES

1. The Agency has adopted the [2021-86 ED Decision on sensitive functions](#) to put in place a policy regarding the identification and management of the sensitive functions. The goal of defining such functions is to prevent fraud, misuse of funds or use of highly sensitive information for personal gain within the EU Institutions/Agencies. This ED decision tasks the Agency to update on a regular basis an inventory of sensitive functions and relevant risks in order to set up controls to mitigate them. The first risk assessment on the sensitive functions was completed in March 2023. The Decision EDD 2021-86 became applicable as of May 2022.
2. The MBD 2021/05 on Anti-Fraud Strategy and its Action Plan includes as an annex reporting template for transmission of alleged fraud as per the established mechanism for reporting irregularities or alleged fraud (section 8 of the MBD 2021/05).
3. The Agency has updated its framework on conflict of interest, by adopting the [Management Board Decision 2021-15 on Conflict of Interests](#). It created a centralised system of conflict of interest declarations, for which the template is provided as an annex to the decision. Also, it established an Ethical Committee, which is available to the Management Board, Executive Director and to the Heads of Units for consultation on matters related to potential conflict of interests

---

<sup>3</sup> Available under the following link: [https://inet/css/hr/docs/HR%20Forms/Recruitment/COI%20form\\_template.docx](https://inet/css/hr/docs/HR%20Forms/Recruitment/COI%20form_template.docx)

<sup>4</sup> Available under the following link: <https://inet/css/hr/docs/HR%20Forms/Recruitment/Declaration%20conflict%20of%20interest%20Art.11.docx>

of the individuals in relation to the Agency and its bodies. The Ethical Committee is composed of the Head of the Executive Director's Office Unit (EDO), acting as the Chair of the Committee, of the Head of Corporate Support Services Unit (CSS) and of the Agency's Legal Adviser.

4. Following the ENISA's Internal Control assessment for the year 2021, as well as guidance on Internal Controls obtained via the EU Agencies network, the Agency has reviewed its Internal Controls framework ([MB Decision 2019-12 on internal controls framework](#)). By means of the [Management Board Decision 2022-11](#), the list of Internal Control Indicators has been updated with a view to address the Agency's organisational changes, increase effectiveness and ensure the proper implementation of the Internal Control Framework. The annual Internal control Assessment exercises for 2022 and 2023 have been conducted based on the revised Internal Control framework.
5. Following ENISA's Financial Rules ([Management Board Decision 2019-08 Financial rules](#)), the Agency shall ensure that all significant deviations (exceptions) from regulations, policies, procedures and decisions of the Management Board or the Executive Director are registered and, reported to the Management Board and Discharge Authorities in accordance with the principle of transparency. In this regard, there is a revised [2023-102 ED Decision on Registry of exceptions](#) in force. It clarifies the notion of "exception" and set up the process for registering exceptions. The template for staff to register an exception is shared on the compliance collaboration iNet page and the ARES workflow is created with the instruction on how to register an exception.
6. The Agency has implemented ARES tool for document management and adopted the [ENISA Document Management Policy](#). To enhance data security, in particular, a secure mail system, [ENISA email policy](#) has been adopted.

### 3. OVERVIEW OF THE HANDLING OF CASES

This section contains an enumeration of sensitive cases handled during the period 2021-2024.

In the course of 2021-2024, the Agency has dealt with the following OLAF cases:

1. OC/2022/0086
2. OC/2020/0942/A1 as a split from case OC/2018/0598/A1
3. OC/2022/0129
4. OC/2023/1207

The Agency has initiated the following preliminary assessments/administrative inquiry procedures (respective Executive Director's Decisions remain confidential):

1. EDD 18/2022
2. EDD 41/2022
3. EDD 44/2023 EDD 13/2024

The EDO Compliance Sector and Anti-fraud Coordinator /Legal Adviser have been involved as required in the relevant cases.

It is to be noted, that the Agency has carried out all actions previously requested by the European Anti-Fraud Office and no obligations, follow-up actions or recommendations are pending.



## 4. WAY FORWARD

For the 2025-2027, the following actions are proposed to be included in the Action Plan to be included in the Anti-Fraud strategy for the next 3-years period so to achieve a goal of the fraud free working environment:

1. The Agency will keep organising yearly two trainings: a general one addressed to all staff members and a more specialised one addressed to middle managers, with cooperation with the OLAF expert.
2. Compliance in the areas of procurement and recruitment specifically will be monitored, also considering relevant case law and recommendations of auditors (ECA, IAS) and specifically with regard to the management of conflicts of interest.
3. Policy on remunerated expert will be endorsed and published in iNet for all staff so to avoid discrepancies and exceptions registered while using the CEI list.
4. Quarterly monitoring of the agency legal production by compliance sector in cooperation with the CSS/HR.
5. Dedicated trainings to the for project managers for achieving a better understanding of finance responsibilities so as for members of selection panels along with the guidelines on how to duly manage potential conflict of interest situations.