EUROPEAN UNION AGENCY FOR RAILWAYS

Moving Europe towards a sustainable and safe railway system without frontiers.

ERA
ANTI FRAUD STRATEGY (AFS)
2025-2027

Contents

1. General background

The European Union Agency for Railways (ERA) is responsible for ensuring the safety, interoperability, and enhanced performance of the European railway system. In its regulatory and oversight capacity, ERA manages complex technical and financial responsibilities that expose it to various fraud risks. To safeguard the integrity of its operations and ensure the efficient and transparent use of public funds, ERA must develop a comprehensive anti-fraud strategy (AFS).

Key concepts

A clear understanding of fraud and irregularity is crucial for defining the objectives and the scope of the AFS.

In the context of the EU, *fraud* is generally defined as any intentional act or omission involving deception to secure an unjust or illegal gain, particularly with respect to the misuse of EU funds[1].

Irregularity, on the other hand, refers to any breach of applicable law, regulation, or contractual obligation that leads to improper expenditure of EU funds. Unlike fraud, which involves intent and deceit, irregularities can occur due to noncompliance with established procedures. These failures to follow procedures or guidelines may happen even without any fraudulent intent. Although irregularities do not involve deceit, they still jeopardise the proper use of EU resources and require correction. Within the Agency, irregularities are managed through procedures for monitoring exceptions and non-compliance events (i.e. nonconformities).

The key difference between fraud and irregularity is the component of intent which is absent in irregularities. Consequently, irregularities fall outside the scope of the AFS.

At its core, fraud is about deception—when an individual seeks to gain value through dishonest means. For instance, it is akin to someone trying to sneak a free ride on a train. Although such actions might seem trivial to some, they undermine the integrity of the entire system. In the context of the ERA, fraud can divert crucial resources away from rail projects that benefit the public, adversely affecting safety, service, and innovation.

This highlights the importance of ERA's AFS which serves as a safeguard against attempts to misuse funds or resources. The strategy emphasises not only adherence to rules and regulations but also the cultivation of a culture of integrity and trust within ERA and its stakeholders.

EU regulatory framework context and expectations from the AFS

ERA operates within the broader regulatory framework of the European Union, which places a strong emphasis on transparency, accountability, and integrity among all public bodies. Regulation (EU) 2016/796 outlines ERA's roles and responsibilities, incorporating provisions that align the Agency with these principles. As part of the EU institutional framework, ERA is expected to establish robust mechanisms for the prevention, detection, and response to fraud, in accordance with the EU's zero-tolerance policy toward fraud.

Moreover, ERA collaborates with various EU bodies, including the European Anti-Fraud Office (OLAF), to mitigate fraud risks comprehensively. OLAF's mandate is to investigate fraud against the EU budget and serious misconduct of EU staff or other servants of the Union, and its guidelines serve as a baseline for ERA in developing its anti-fraud strategy.

Inherent risks of fraud in ERA

As a decentralised EU body, ERA is susceptible to numerous fraud risks, including conflicts of interest, procurement fraud, financial mismanagement, and data manipulation. ERA's role for authorising rail vehicles, certifying rail operators and granting European Railway Traffic Management System (ERTMS) trackside approvals across the EU requires collaboration with multiple stakeholders, such as national rail authorities, private sector companies, and contractors. This extensive network can heighten the risk of unethical

[1] ECA Special Report – Fighting fraud in EU spending: action needed

behaviour, procurement irregularities, or manipulation of certification processes. The complexity of ERA's operations encompassing technical standard-setting, cooperation with national rail regulators, and extensive procurement activities creates potential vulnerabilities. Additionally, the increasing threats of cyber-attacks and data breaches necessitate a strengthened internal control system. It is essential for ERA to establish a dedicated AFS to identify and address any gaps, thereby safeguarding the integrity of the Agency's work.

By addressing these risks, ERA ensures that its regulatory decisions are unbiased, transparent, and compliant with EU rules.

Internal control framework and alignment with the EC Antifraud strategy

ERA's anti-fraud strategy is embedded within its overall Internal Control Framework (ICF), which aims at ensuring compliance, operational efficiency, and protection of EU financial interests. Fraud risk management is a vital element of this framework. The European Commission's Anti-Fraud Strategy (CAFS) highlights a structured approach to cooperation among EU institutions, focusing on collective efforts to prevent and combat fraud. This collaboration is crucial for maintaining the integrity of the EU budget and enhancing the overall effectiveness of anti-fraud measures. The strategy encourages and promotes best practices and standards for approaching antifraud in decentralised bodies

By aligning ERA's anti-fraud measures with the European Commission's overarching goals, ERA ensures consistency in managing fraud risks and adherence to the EU's strict standards of accountability. ERA's AFS is a fundamental component of its ICF, prioritizing early detection, risk-based prevention, and efficient responses to fraud incidents, to fully protect the EU budget.

2. Specific context of European Union Agency for Railways

Having outlined the **general background** and key principles that shape ERA's AFS, it is important to turn our attention to the **specific areas of operation** where the Agency faces heightened fraud risks. While Section 1 provided an overarching understanding of fraud and irregularities, as well as ERA's role within the broader EU regulatory framework, the next section focuses on the concrete operational domains within ERA that are most vulnerable to fraud.

ERA's core mission is to uphold the highest standards of railway safety and interoperability across the EU. As such, its key operational activities are vital to the European rail system's efficiency and security. However, these areas are not without significant fraud risks**,** which, if left unchecked, could undermine ERA's work, damage its reputation, and compromise public safety. In particular, ERA's core responsibilities—such as safety certification, vehicle authorization, ERTMS trackside approval, data management, financial oversight, and human resources—present a range of fraud risks that need targeted mitigation. Each of these areas is characterized by complex procedures, significant financial and political implications, and interactions with numerous stakeholders, all of which heighten the potential for fraud.

Safety certification, vehicle authorisation and ERTMS trackside approvals

ERA is responsible for ensuring the upholding the highest standards of railway safety within the EU. The certification, authorisation and approval processes involve significant financial and political factors which can create vulnerabilities to fraud, corruption or bribery. Thus, the certification process should be viewed as a high-risk area, as fraud could undermine safety and interoperability, compromise rail operations, and damage ERA's credibility. Therefore, implementing measures against conflict of interest and collusion is critical.

Data and digitalization

As ERA increasingly focuses on data management and the digitalization of railway systems, it manages vast amounts of sensitive information, including data on rail safety, vehicle authorizations, and technical standards. As the custodian of this data and being dependant on digital platforms, ERA is at risk of cyber fraud, unauthorized access to sensitive information. Implementing robust information security protocols, regular cybersecurity training for staff, and tighter access controls to sensitive systems and data should be emphasised. Protecting digital assets and establishing strong (cyber)security protocols to prevent both internal and external fraud attempts represent a priority.

Financial, procurement and contract management

ERA operates within the EU budget framework, which allocates substantial funds for operational expenses. Its annual budget is approximately 40 million euros, with 70% sourced from EU contribution, 28% from fees and charges and 2% from EFTA countries that participate in the Agency's work. Given the diverse funding sources, vigilance against procurement fraud and financial mismanagement is essential. Effective resource management requires strict compliance with the financial regulation to prevent fraudulent use of funds, overbilling, or the misuse of resources. In addition, effective contract management is essential to ensure that obligations are met, and contracts are executed per agreed terms, thereby minimizing the risks of fraud, delays, and cost overruns.

Continuous monitoring of budget execution and contract performance is crucial for ensuring that funds are used efficiently and in accordance with EU financial rules. Inadequate monitoring and reporting of contract performance can obscure fraudulent activities, making it challenging to detect irregularities. Strong oversight of contract management processes will aid in the early identification of potential risks and ensure that corrective actions are taken, thereby reducing vulnerabilities to fraud and safeguarding ERA's financial integrity.

HR management

As ERA's staff grows in a multicultural and multilingual environment, effective management of human resources becomes increasingly important[2]. Approximately 73% of the budget is allocated to staff expenditures (including salaries, allowances, missions etc). Changes in the organisational culture such as a shift towards remote work introduce new dynamics on how work is conducted, monitored and managed, which may create vulnerabilities. To maintain the integrity of ERA's human resource management in this evolving work environment, robust whistleblowing mechanisms can help compensate for reduced face-to-face interactions.

Also, remote work heavily relies on digital platforms for communication, collaboration, and executing transactions. This dependence increases the risks of cyber fraud, phishing attacks, data breaches, and unauthorized access to sensitive information. This dependence also applies in the area of HR recruitment, where remote interviews of candidates are often used and the negative impact of artificial intelligence (AI) in the recruitment process (e.g. unethical AI assistance such as use of AI tool for real time assistance during remote interviews/written test, providing answers or prompts to the candidate or AI tool used to forge or tamper with official documents submitted during the application process) should not be underestimated.

[2] 148 staff members (148TA & 30 CA) at the expiration of the previous Antifraud Strategy to 201 staff members – 163 TA & 35 CA + 3 SNEs when this strategy is approved.

3. Methodology

The above-mentioned areas could expose the Agency to fraud risks. These risks—ranging from conflicts of interest in certification processes to vulnerabilities in cyber fraud and procurement irregularities—must be mitigated through a comprehensive and systematic approach.

To effectively address these risks, ERA's AFS must be grounded in a clear, structured methodology. This methodology is not only designed to identify and prioritize fraud risks, but also to implement preventive, detective, and corrective measures that ensure integrity across ERA's operations. This section outlines the methodology used to develop and implement the AFS, with a particular focus on prevention, risk assessment, and collaborative efforts that foster ethical behaviour across all stakeholders.

The methodology underpinning the AFS aligns with the **OLAF Methodology**[3] and focuses on both preventive and corrective measures. It includes evaluating the effectiveness of current anti-fraud measures, identifying and assessing risks, and setting clear objectives to safeguard ERA's operational integrity. The following section delves into the evaluation of ERA's previous AFS to assess its strengths, identify gaps, and highlight areas that need further attention in light of the evolving fraud landscape.

The actions cover all stages of the anti-fraud cycle emphasizing prevention over correction. For instance, ERA prioritizes training and awareness to ensure that all staff members know what to observe and how to report any suspicious activities. Additionally, the AFS includes detection measures; similar to train ticket checks that confirm fare payment, ERA employs monitoring and ex-post controls systems/checks to identify irregularities early on. If fraud occurs, the AFS delineates clear pathways for correction, enabling ERA to address issues quickly and effectively.

Collaboration is essential to ERA. By engaging stakeholders, ERA fosters a culture of collective responsibility for upholding ethical standards. This joint effort builds trust and ensures that resources are utilized wisely for the benefit of all.

4. Evaluation of the previous AFS

The previous ERA's AFS focused on three main objectives:

- Effectively managing conflicts of interest and promoting ethical values

The objective was achieved by developing a 'positive' approach to conflict of interest. Measures included implementing a system of annual submission of declarations of interests facilitating informed assessment and increasing transparency for external stakeholders. This system is tailored to address the ERA's fraud risk exposure. Additionally, customised training sessions on ethics and separately on antifraud target the entire anti-fraud cycle including detection, prevention, investigation, and correction. However, due to the evolving nature of fraud (e.g. cyber threats) as well as the adaptation of the Agency to new technologies, ongoing awareness is essential to keep staff informed about the latest threats and fraud techniques thereby enhancing their understanding of emerging fraud risks.

- Ensuring that fraud suspicion is properly managed

The objective has been achieved through adopting the whistleblowing rules and by raising awareness about the various ways to report suspicions of fraud. This has been accomplished via training sessions and guidelines on reporting fraud suspicion. It is essential to continue these efforts in the new AFS to encourage staff to report any fraud suspicions. This not only helps deter potential fraudsters and enables early detection of fraudulent activities but also fosters a culture of honesty and integrity, where ethical behaviour is the norm

[3] OLAF Methodology and guidance for the anti-fraud strategies of EU Decentralised Agencies and Joint Undertakings - Ref. Ares (2024)4040978 – 05/06/2024

(ensuring alignment with the objectives of the 'Better together' project, which is focused on ensuring a positive organisational culture at ERA).

› Enhance data documentation and security

The objective has been partially achieved as the IT security environment and associated threats are in a state of continuous evolution. Consequently, fully addressing this risk remains a challenge and a priority in the new AFS as well. ERA has implemented security measures to ensure data integrity, including strict access controls to prevent unauthorised individuals from accessing sensitive information and it regularly updates its IT security plans. Additionally, ERA has also put in place measures to protect its information assets and systems while developing a systematic internal awareness of IT security risks. These measures will continue in the new AFS due to the evolving threat landscape. Regular updates and improvement to security measures will enable the Agency to adapt to the latest fraud technologies thereby building trust with the stakeholders who depend on the Agency to safeguard their data and information. The Agency is developing an Information Security management system to ensure that that the confidentiality, integrity and availability of its information assets are protected at the required level.

The evaluation of ERA's previous Anti-Fraud Strategy reveals that while significant progress has been made in managing conflicts of interest**,** reporting fraud suspicion**,** and enhancing data security**,** there is a clear need to further adapt these measures to the rapidly changing fraud environment, including growing cyber threats. By reflecting on the achievements and limitations of the previous AFS, ERA can ensure that its new strategy remains responsive to emerging fraud risks, particularly in the areas of digitalization and evolving work environments.

5. Anti-fraud measures in place in ERA

Building on the evaluation of the previous Anti-Fraud Strategy, ERA has implemented a robust set of anti-fraud measures that focus on prevention, detection, and investigation. These measures are embedded within the Agency's Integrated Management Control System (IMCS) and align with the European Commission's Internal Control Framework (ICF).

The following section provides a detailed overview of these measures:

Prevention measures:

› Framework of Good Administration behaviour which includes a code of conduct, rules on conflict of interests and in particular the obligation for all staff members to submit annual declarations of interest (MB DECISION n°199 adopting the revised Framework for Good Administrative Behaviour);
› Annual declarations of interest for Management Board members and independent experts (MB DECISION n°162 for the prevention and management of conflicts of interest);
› Procedure for screening the Declarations of Interests (DoI);
› A transparency policy, whereby CVs and Declarations of Interest (DoIs) of Management Board members and middle and senior management are published to enable public scrutiny;
› Whistleblowing policy for staff for reporting improprieties (MB DECISION n°183 on the guidelines on whistleblowing);
› Mandatory customised and comprehensive trainings on ethics and antifraud in a four year cycle covering all staff members (and induction sessions on ethics for newcomers)
› Annual risk assessment, which considers also the risk of fraud

Detection measures:

› Ex-ante and ex-post controls in financial and non-financial areas whenever the management finds its necessary to manage a specific risk
› IT tools to prevent unauthorized access to IT systems and monitor IT security

Investigation measures

› Rules for providing full cooperation with OLAF in case of investigations (Decision no 8 of the Administrative Board of ERA concerning terms and conditions for internal investigations in relation to the prevention of fraud, corruption and any illegal activity detrimental to the Communities' interests)

Cooperate with EPPO by providing access to documents, supporting investigation and data exchange in order for preventing, detecting and prosecuting financial crimes affecting ERA's budget

6. Roles and responsibilities

Implementing anti-fraud measures requires clear accountability and coordinated efforts across the Agency. The success of the AFS depends on the roles and responsibilities of various stakeholders, from leadership and oversight to specialized units and staff members.

This section outlines how each entity within ERA contributes to fostering a culture of ethical behaviour and fraud prevention, ensuring that the AFS is effectively executed and sustained across all levels of the organization.

Leadership and oversight

Management Board (MB):

- Approves the Anti-Fraud Strategy (AFS) and provides overall oversight.

Executive Director (ED):

- Establishes a strong commitment to ethical behaviour and a zero-tolerance policy for fraud.
- Ultimately accountable for the implementation of the AFS.

Management Team (MT):

- Regularly discusses and agrees on mitigating measures for risks impacting projects and services, including fraud risks (e.g. Monthly Management Review Report).

Risk Management and Internal Control

Manager in Charge of Risk Management and Internal Control (RMIC):

- Coordinates the implementation of the internal control framework including AFS
- Coordinates fraud risk assessment and regularly follow on the actions

Heads of Units/Department:

- Promote an anti-fraud culture within their respective areas of responsibility.
- Must ensure that main fraud risks at their level of responsibilities are known and adequately managed

"Specialised" units/functions

- **Corporate Assurance and Performance Unit (CAP)**:
  - Implements and maintains internal controls over financial reporting and transaction processing.
  - Analyzes financial data to detect red flags indicating potential fraud.
- **Ethics Officer & OLAF contact point**:
  - Integrates ethical considerations into all business processes.
  - Organizes training sessions on fraud awareness and reporting.
  - Assists OLAF in investigating reported fraud suspicions.
  - Provides advice on ethical management and potential conflicts of interest.
- **Legal Officer**:
  - Identifies and prevents risks related to breach of legal provisions.
- **Human Resources Unit (RSU)**:
  - Supports the creation of a culture of trust through dedicated training and awareness-raising campaigns.

- **Information Technology team (ITFM)**:
  - Implements measures related to IT security and cybersecurity

In this collaborative environment, **all staff members** play a crucial role in implementing the AFS and fostering an organizational culture that leaves no room for fraud. However, effective implementation also hinges on understanding the specific fraud risks that ERA faces.

7. Fraud Risk Assessment

ERA's Integrated Management Control System (IMCS) includes a dedicated procedure for identifying and assessing potential fraud risks associated with administrative and operational business processes. Identified risks are managed according to the corporate risk appetite and mitigation actions are monitored and reported as part of the annual internal control assessment.

Based on the fraud risks assessment, ERA has prioritised the following risks for the AFS:

1. Failure to detect or report fraud due to insufficient staff awareness of the latest fraud tactics/lack of confidence in the whistleblowing mechanisms due to:

  - *potential inadequate training on emerging fraud risks/ lack of a well communicated and trusted whistleblowing system,*

› which in return may lead to:

  - *undetected or delayed detection of fraud, resulting in prolonged financial loss or reputational damage,*
  - *underreporting of suspicious activities due to fear of retaliation or lack of trust in the process and increased risk exposure,*
  - *increased risk exposure to high-risk areas such as financial transactions and contract management*

The impact may be significant: financial loss due to undetected fraud, damage to the Agency's integrity and culture if fraud is allowed to persist without detection and reporting.

Overall risk level: significant

2. Unauthorised access to IT systems leading to data breaches and failure to detect and mitigate emerging cyber threats in real time due to:

  - *Inadequate cybersecurity protocols, lack of staff awareness of cybersecurity best practices, weak access control measures,*

› which in return may lead to:

  - *data breaches leading to the loss of sensitive information,*
  - *disruption of business operations due to cyberattacks.*

The impact may be significant: financial losses, long term reputational damage, loss of critical/sensitive data

Overall risk level: significant

3. Manipulation of internal controls to approve unauthorized payments, misappropriate funds, or deliver substandard services/goods without detection (e.g., false invoicing, contract kickbacks, collusion between vendors and staff. due to:

  - *potential inadequate internal control, lack of oversight in financial transactions, weak contract monitoring*

› which in return may lead to:

- *potential payments, misappropriation of funds, overpayments for substandard services or good*

The impact may be significant: misallocation of resources and potential budget overruns, reputational damage.

Overall risk level: moderate- significant

4. Failure to detect fraudulent behaviour due to insufficient use of technology due to:

- *Lack of modern tools for fraud detection (ie. data analytics, artificial intelligence based systems), resistance to adopting new technologies or lack of staff training in using them,*

› which in return may lead to:

- *delayed detection of fraudulent activities, increasing financial and reputational harm;*
- *difficulty in identifying complex or large-scale fraud schemes*
- *lost opportunities to proactively prevent fraud through real-time monitoring.*

The impact may be significant: financial losses due to prolonged fraudulent activities going undetected, long term reputational damage, damage to the Agency's reputation as fraud may appear unchecked.

Overall risk level: significant

These risk areas have been prioritised by considering specific threats and vulnerabilities, as well as scenarios in which fraud could occur without effective mitigation measures. The identification of these critical risks underscores the need for targeted objectives to enhance ERA's anti-fraud efforts.

8. Objectives

In response to the identified priority areas, ERA has established three main strategic anti-fraud objectives:

Objective 1 *Enhance and sustain a strong ethics and antifraud culture through improved training programs and the enhancement of antifraud information provided to staff*

In light of the current fraud risk environment, fraud deterrence remains the most effective approach to combatting fraud, particularly by disseminating ethical standards and relevant rules governing ERA's activities. ERA is already implementing mandatory anti-fraud and ethics training sessions, which should be continued and improved. The focus should be on real case scenarios, current fraud risks and the identification of red flags in everyday work. These training sessions must be updated annually to incorporate regulatory changes, emerging fraud trends, or new internal control mechanisms.
Additionally, staff members should have access to up-to-date information on all relevant anti-fraud policies/procedures/guidelines along with clear instructions on how to report fraud anonymously and securely and lessons learned from previous fraud incidents.
Implementing whistleblowing rules and training programs has successfully increased staff awareness regarding the reporting of suspected fraud. This proactive measure is crucial for early detection and deterrence of fraudulent activities. To encourage reporting it is vital to strengthen whistleblower protection and establish clear practical arrangements. Staff should receive comprehensive guidance on reporting serious misconduct to foster a culture of trust within the organisation.

***Objective 2**. Enhance cybersecurity and safeguard data integrity through the implementation of advanced cybersecurity protocols and measures*

The dynamic nature of fraud, particularly with emerging cyber threats, necessitates the implementation of key measures aimed at enhancing cybersecurity and mitigate fraud risks. These measures informed by the requirements of the cybersecurity regulation are essential for securing information systems, reducing the likelihood of cyber-related fraud and ensuring integrity of data and operations. Additionally, the management of access rights to IT systems should be improved by clarifying roles and responsibilities to ensure security and integrity of the system and minimise the risk for data manipulation.

Information campaigns should be organised to raise awareness on cyber risks and prevention measures as the previous strategy has already identified the need for continuous updates to combat these evolving challenges.

***Objective 3**. Strengthen internal controls to prevent and detect fraud with a focus on reducing residual risk in certain areas*

The objective is to establish effective controls and guidance in areas where potential gaps could be exploited. While the internal controls have been assessed as adequate controls to prevent and detect fraud, the AFS will further reduce fraud risks in contract management by enhancing vendor performance against contractual obligations. Moreover, the AFS will enforce clarity and transparency in contract terms particularly regarding payment schedules, deliverable and payment metrics.
ERA will make use of ex-post controls to improve fraud detection, considering cost-benefit factors, and identify appropriate actions to raise awareness among those involved in the ex-ante controls.
The impact of artificial intelligence should be thoroughly assessed, particularly in processes with critical implications such as IT and selection procedures.

These objectives reflect ERA's commitment to addressing the identified fraud risks proactively and systematically, ensuring that the AFS remains robust and effective in safeguarding the integrity of its operations.
To achieve these objectives, a comprehensive action plan is essential (see Annex). The action plan will outline the specific steps and measures needed to implement the objectives effectively, facilitating accountability and alignment across all levels of the organization.

9. Monitoring, reporting and communication

This strategy is valid for three years and might be updated before the end of the implementation, considering the results of future fraud risk assessments.

The AFS action plan will be updated at least once per year to evaluate the degree of AFS implementation and progress will be reported annually as part of the annual internal control assessment and of the Consolidated Annual Activity Report (CAAR).

This ongoing monitoring and reporting mechanism ensures that the effectiveness of the anti-fraud measures is assessed regularly, allowing for timely adjustments to the strategy as needed. By maintaining clear communication and oversight, ERA can continue to foster a culture of accountability and transparency, reinforcing the commitment to ethical practices and the successful implementation of the AFS.

Information on the antifraud strategy will be conveyed to staff during the mandatory training sessions on anti-fraud and the possibility given to staff to provide feedback on the effectiveness of antifraud measures.

As foreseen in the action plan, antifraud messages on specific topics will be conveyed to staff through multiple channels: Agency news, general assembly.

Moving Europe towards a sustainable and
safe railway system without frontiers.

ANNEX - ACTION PLAN

Objective 1: Enhance and sustain a strong ethics and antifraud culture through improved training programs and the enhancement of antifraud information provided to staff					
Related risk	**Sub-objective**	**Action**	**Unit in charge**	**Indicator**	**Target date**
Risk of inadequate staff awareness and preparedness in identifying and managing fraud risks.	1.1 Improve and sustain antifraud and Ethics training programs	1.1.1 Ensure the mandatory antifraud and ethics training program is updated annually to reflect regulatory changes, emerging fraud risks, and new internal control mechanisms.	EDO/CAP (Ethics officer) in cooperation with HR	AFS training updated annually (at least once by end 2025 and then annually depending on the needs) Baseline: 10.4 % in 2024 (separate percentage for each training)	End 2025 As of 2025 (2nd semester).
		1.1.2 Incorporate real-life fraud cases, current fraud risks, and identification of red flags into the training sessions to improve staff's practical understanding of fraud risks in their daily work.		Number of red flags integrated into the training sessions (exact target to be determined once the AFS training material is reviewed) Baseline: NA	
		1.1.3 Ensure that all newcomers receive mandatory antifraud and ethics training as part of their onboarding process to embed ethical standards from the outset.	EDO/CAP (Ethics officer) in cooperation with HR	Percentage of newcomers who complete training during induction sessions (100%) Baseline: 100%	Starting 2025
Risk of ineffective communication and dissemination of antifraud policies, procedures, and guidance across the organization.	1.2 Improve access to antifraud information and guidance	1.2.1 Review the current ethics and antifraud section on the Intranet to ensure that all relevant antifraud policies, procedures and guidelines are updated regularly and easily accessible to all staff.	EDO/CAP (Ethics officer) in cooperation with RSU (Digital team)	Update frequency of content of the ethics and antifraud section on Intranet (at least one update per year) Baseline: 1	Starting with the 2nd semester of 2025 and at least annually after
		1.2.2 Regularly communicate ethics and antifraud messages through internal newsletters, intranet, and staff meetings, ensuring that fraud prevention remains a visible and continuous priority for all staff members, including a stable link with the Better Together project (positive organisational culture)	EDO/RSU/CAP (Ethics officer) in cooperation with SAC team	Percentage of antifraud policies and procedures reviewed annually No. of international information campaigns on a positive and fraud-free organisational culture Baseline: 0	Starting June 2025 and at least annual updates At least 1/year starting 2025

		1.2.3 Create and distribute a comprehensive list of "red flags" for fraud detection, particularly tailored to high-risk areas such as procurement and contract management, as part of ongoing awareness and training efforts	EDO/CAP (Ethics officer) & Legal and procurement team	Completion and distribution timeline of the "red flags" list Baseline: 0	November 2025 – (distribution as of December 2025); to be incorporated in training sessions staring with 2026
Risk of underreporting fraud or failure to report suspicious activities.	1.3 Strengthen whistleblowing mechanisms	1.3.1 Develop and communicate clear, practical guidelines for staff on how to report fraud securely and anonymously. This should include step-by-step instructions and options for both internal and external reporting.	EDO/CAP (Ethics officer)	Completion of guidelines Baseline: 0	December 2025
		1.3.2 Regularly remind staff of the whistleblowing rules, emphasizing the importance of reporting suspicious activities. This shall be done through internal communications (agency news), intranet updates, and antifraud training	EDO/CAP (Ethics officer) in cooperation with SAC team	Reminders about whistleblowing rules Baseline: 2 (during the trainings on antifraud)	Annually

Objective 2: Enhance cybersecurity and safeguard data integrity through the implementation of advanced cybersecurity protocols and measures					
Related risk	**Sub-objective**	**Action**	**Unit in charge**	**Indicator**	**Target date**
Risk of cybersecurity breaches due to inadequate or outdated security measures (exposure to cybersecurity threats)	2.1 Implement advanced cybersecurity protocols	2.1.1 Implement advanced cybersecurity solutions such as firewalls, intrusion detection systems (IDS), encryption, and AI-based monitoring to detect and mitigate cyber threats in real time	RSU (Cybersecurity officer)	Percentage of cybersecurity solutions fully implemented (100%) Baseline: NA	End 2025 -and regular updates after
		2.1.2 Organise regular internal and external cybersecurity audits to evaluate vulnerabilities and ensure that security protocols are up to date and compliant with the latest regulations and best practice	RSU (Cybersecurity officer)	Number of cybersecurity audits completed annually (at least one) Baseline: NA	First audit within 6 months post-implementation of the advanced cybersecurity solutions, followed by periodic audit
Risk of unauthorized access to critical systems (exposure to fraud and data manipulation)	2.2 Secure access to IT systems	2.2.1 Ensure that multi-factor authentication (MFA) is mandatory for all access points to critical systems to reduce the risk of unauthorized access and data manipulation	RSU	Number of IT systems protected by MFA (100%) Baseline: NA	Complete rollout within 6 months for all systems, with continuous monitoring and updates to MFA protocols annually
		2.2.2 Conduct periodic reviews and updates of user access rights to ensure that access privileges are aligned with staff members' current roles and responsibilities, and remove access for any inactive or former employees	RSU for coordination & each business owner responsible for the IT systems	Frequency of user access reviews conducted Baseline: 1	Annually or as needed when there are major organisational changes
Risk of staff negligence or lack of awareness regarding cybersecurity threats	2.3 Raise awareness to staff on cyber risks	2.3.1 Provide regular training and awareness programs on cybersecurity risks and prevention measures	RSU (Cybersecurity officer)	Percentage of staff trained annually on cybersecurity risks (at least 80% by end 2027) Baseline: NA	At least annually
Risk of insufficient integration of external	2.4 Strengthen collaboration with	2.4.1 Collaborate with external cybersecurity experts (particularly CERT_EU and other EU cybersecurity networks) to receive guidance on new threats, technologies, and regulatory requirements. Use this collaboration to strengthen internal cybersecurity defences.	RSU (Cybersecurity officer)	Information sharing session on	At least twice a year

advice/guidance on cybersecurity into internal practices.	external cybersecurity experts			threats/guidance or regulatory requirements Baseline: NA	

Objective 3: Strengthen internal controls to prevent and detect fraud with a focus on reducing residual risk in certain areas					
Related risk	**Sub-objective**	**Action**	**Unit in charge**	**Indicators**	**Target date**
Risk of inadequate oversight and detection of non-compliance or fraud in contract management processes.	3.1 Implement and strengthen ex-post controls	3.1.1 Develop a framework for regular ex-post controls to evaluate vendor compliance with contract terms (i.e. review financial transactions, payment schedule and deliverables etc)	CAP (budget team and ICC)	Number of ex-post control performed annually Baseline: NA	June 2025 to establish the framework (ex-post controls to begin immediately after; periodicity to be defined in line with the framework)
		3.1.2 Provide training and awareness session for staff involved in contract management**.** These training sessions should cover key fraud risks, red flags in contract management and highlight the importance of thorough vetting and due diligence before approving deliverables	Legal and procurement team in cooperation with the Ethics officer	Percentage of contract managers trained on fraud risks (100 %) Baseline: NA	By June 2025 (training to be developed and first session delivered) Annually (for delivering the training sessions)
Risk of inadequate contract performance monitoring and enforcement incresaing vulnerability to fraud	3.2 Enforce clarity and transparency in contracts	3.2.1 Standardise and enforce transparent contractual terms, particularly regarding payment schedules, deliverables, and payment metrics. Contracts should have clear, measurable, and enforceable performance indicators to reduce ambiguity and fraud risk	Legal and procurement team in cooperation with CAP	Number of contractual disputes related to ambiguous terms (trend to zero) Baseline: NA	October 2025 followed by ongoing monitoring and updates as needed
Risk of inadequate adaptation to evolving fraud risks and operational changes	3.3 Evaluate and update internal control systems	3.3.1 Perform regular reviews of internal control systems to identify any potential gaps that could be exploited. Update controls based on lessons learned from previous fraud incidents, audit findings, and changes in the regulatory or operational environment.	IMCS team in cooperation with the process owners	Frequency of internal control reviews/assessment conducted Baseline: 0	Assessment every 12 months starting in March 2026
Potential for ineffective fraud detection and response due to inadequate understanding and implementation of AI technologies	3.4 Assess the Use of AI for Fraud Detection	3.4.1 Explore the possibility of conducting an impact assessment to evaluate how AI can be leveraged for fraud detection, particularly in areas like IT, procurement, and selection procedures.	RSU + MARS	Completion of AI Impact assessment Baseline: NA	1st quarter 2026