EUROPEAN PUBLIC PROSECUTOR'S OFFICE

College Decision 018/2025

DECISION OF THE COLLEGE OF THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE OF 26 FEBRUARY 2025

AMENDING DECISION 043/2021 OF THE COLLEGE OF THE EPPO OF 12 MAY 2021 ON THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE ('EPPO') RISK MANAGEMENT POLICY

The College of the European Public Prosecutor's Office ('the EPPO'),

Having regard to Council Regulation (EU) 1939/2017 of 12 October 2017[1], implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('EPPO'), hereinafter "the EPPO Regulation",

Having regard to Decision 002/2021 of the College of the European Public Prosecutor's Office on the Financial Rules applicable to the EPPO, as amended by the Decision 023/2023 of the College of the EPPO of 19 April 2023, hereinafter referred to as "EPPO's Financial Rules", and in particular Article 30(3)(b), Article 30(4)(a) and Article 45(2) thereof,

Having regard to the Implementation Guide on Risk Management in the Commission (version 2018-2019), based on the Communication of the European Commission on Risk Management[2].

Whereas:

1. In accordance with Article 30(3)(b) of the EPPO's Financial Rules, "Effective internal control shall be based on best international practices and shall include an appropriate risk management and control strategy that includes control at recipient level."

[1] OJ L 283, 31.10.2017, p. 1–71
[2] SEC(2005)1327

2. In accordance with Article 30(4)(a) of the EPPO's Financial Rules, "Efficient internal control shall be based on the implementation of an appropriate risk management and control strategy coordinated among appropriate actors involved in the control chain."
3. In accordance with Article 45(2) of the EPPO's Financial Rules "The authorising officer shall put in place the organisational structure and the internal control systems suited to the performance of the duties of authorising officer, in accordance with the minimum standards or principles adopted by the College, on the basis of the Internal Control Framework laid down by the Commission for its own departments and having due regard to the risks associated with the management environment, including where applicable specific risks associated to decentralized offices, and the nature of the actions financed. The establishment of such structure and systems shall be supported by a comprehensive risk analysis, which takes into account their cost-effectiveness and performance considerations.

Has adopted this Decision:

Article 1

The Annex to the Decision 043/2021 of the College of the EPPO of 12 May 2021 on the European Public Prosecutor's Office ('EPPO') Risk Management Policy is hereby amended and replaced by the Annex to this Decision, which forms an integral part of this Decision.

Article 2

This decision shall take effect on the day following that of its adoption.

Done at Luxembourg on 26 February 2025.

On behalf of the College,

Laura Codruța KÖVESI

European Chief Prosecutor

Qualified electronic signature by:
LAURA CODRUȚA KÖVESI
Date: 2025-03-07 15:19:19 +01:00

Annex

RISK MANAGEMENT POLICY OF THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE ('EPPO')

Contents

1. Definitions and concepts

1.1. What is a risk?

A risk is defined as any event or issue that could potentially occur and adversely impact the achievement of the EPPO's political, strategic, and operational objectives.

Risks can be associated with the EPPO's:

- **Specific Management Objectives**: Related to the detailed goals set out in specific projects or operational plans.
- **Organisational Management Objectives**: Pertaining to the overall governance, structural integrity, and administrative functions of the EPPO.
- **Implicit Objectives**: Such as protecting staff, safeguarding assets, and securing information.

1.2. What is Risk Management?

Risk Management is defined as: "A continuous, proactive and systematic process of identifying, assessing, and managing risks in alignment with the accepted risk levels, carried out at every level of the EPPO to provide reasonable assurance regarding the achievement of the organization's objectives".

Practically, Risk Management involves:

- **Identification and Assessment**: Identifying and carefully assessing potential problems that could impact the execution of the organization's activities and the achievement of its objectives.
- **Prioritization**: Prioritizing risks according to their relative significance, typically measured in terms of potential financial impact and other impacts.
- **Mitigation Actions**: Taking actions to reduce risks to a level deemed acceptable by management.

Reducing risk to zero is generally unfeasible and rarely cost-effective. A certain degree of risk acceptance is necessary to keep the organization dynamic and responsive to opportunities and changes.

Risk Management is largely common sense: every manager naturally considers and manages potential problems that could affect their activities and objectives. However, the approach set out in this document aims to make the EPPO's Risk Management a continuous, systematic, and structured exercise, ensuring that it is consistently applied across the organization.

1.3. Integration of Risk Management in the EPPO

Risk Management should not be a one-off or annual bureaucratic exercise. The level of resources and documentation devoted to it should vary depending on the criticality of the activity, ranging from formal reviews and risk management plans for major activities to simple recording of risks for everyday work.

1.4. Risk Management Key Responsibilities

All individuals involved in performing an activity should also assess and manage the risks associated with it. Within this overarching framework, different actors play specific roles at various hierarchical levels:

- **European Chief Prosecutor**: The European Chief Prosecutor, as Head of the Office according to Article 11 of the EPPO Regulation, is ultimately responsible for the organisation of the work of the EPPO and the direction of its. In this capacity, he/she must ensure that the EPPO's critical risks[3] are identified and appropriately managed.
- **The College**: The College, considering its role under Article 9(3) of the EPPO Regulation, is kept informed of critical risks affecting the EPPO, as required by the Internal Control Principles. This ensures that the highest levels of the organization are aware of and can respond to significant risks.

[3] A **critical risk** is one that poses a significant threat to the organization's objectives, operations, or reputation. Such risks require immediate attention and include those that could disrupt major policy goals, cause legal or financial damage, endanger staff safety, or harm the EPPO's public image.

- **European Prosecutors:** European Prosecutors play a key role in risk identification and mitigation, particularly concerning the EPPO's decentralised offices established in their Member States.
- **Administrative Director**: As legal representative of the EPPO for budgetary and administrative purposes and authorising officer, according to Article 19 of the EPPO Regulation, the Administrative Director is responsible for establishing the organisational structure and internal control systems necessary for performing its duties, in accordance with the minimum standards or principles adopted by the College (Article 45(2) of the EPPO's Financial Rules). This role includes assigning responsibilities, and making decisions on the treatment of critical risks in articulation with the European Chief Prosecutor.
- **Managers and Members of Staff**: Managers and members of staff are responsible for managing risks related to their primary activities and objectives. They play a crucial role in identifying, assessing, and mitigating risks within their areas of responsibility.
- **Internal Control Officer**: The Internal Control Officer supports managers in establishing a coherent and effective Risk Management process within their units. This role involves facilitation, support, and monitoring. The Internal Control Officer ensures that the risk management practices are consistent and effective across the organization.
- **Internal Audit Capability (IAC)**: The IAC conducts independent regular assessments and provides recommendations for improving the effectiveness of risk management, control, and governance processes. The mission and objectives of the IAC are detailed in the Internal Audit Charter. The IAC's independent reviews help ensure that risk management practices are robust and aligned with organizational goals.

1.5. Risk Management and the Internal Control Principles

Risk Management is an essential component of effective internal control. While the 17 Internal Control Principles (ICPs) of the Internal Control Framework of the EPPO[4] represent fundamental management principles, Risk Management enhances the creation of sector/unit-specific internal control environments and strategies, concentrating on activities and domains with the highest risks. Risks can be both financial and non-financial, and non-financial risks can also pose significant threats to the EPPO.

Risk Management supports the application of the ICPs by:

[4] EPPO College Decision 018/2021 on the Internal Control Framework

- **Identifying High-Risk Areas**: Focusing attention and resources on the activities and domains that represent the highest risks to the organization.
- **Tailoring Controls**: Facilitating the development of internal controls that are specific to the identified risks, ensuring that control measures are both relevant and effective.
- **Enhancing Decision-Making**: Providing valuable insights that inform strategic and operational management decisions, leading to better risk-informed decisions across the organization.

By integrating Risk Management into the ICPs, the EPPO ensures a robust and dynamic internal control system that is adaptable to emerging risks and challenges, ultimately supporting the EPPO's objectives and safeguarding its assets and reputation.

1.6. Risk Management

Heads of Sector/Unit are strongly encouraged to assess risks whenever necessary, particularly in the following scenarios:

- **Reorganisation of the Sector/Unit**: Structural changes within the Sector/Unit may introduce new risks or alter existing ones.
- **Staff Changes in Crucial Positions**: Changes in key management or specialist staff can impact the Sector/Unit's risk profile.
- **External Events**: Events such as budget/financial crises, pandemics, or natural disasters can introduce significant new risks.
- **New Legislation**: Changes in laws or regulations can create new compliance risks.
- **Failure of Risk Management**: Identifying and addressing failures in existing Risk Management practices, especially concerning critical risks.

Risk Management should be a regular agenda item in management and Sector/Unit meetings. This practice allows for continuous monitoring of how risks are being managed and enables prompt responses to changes in risk exposure.

Although Risk Management is a continuous exercise and regular monitoring can be informal, formal documentation and review are mandatory at least once per year. Heads of Sector/Unit are required to submit their list of critical risks as part of the Single Programming Document exercise. Additionally, Heads of Sector/Unit should report any newly identified critical risks on an ad-hoc basis throughout the year.

2. The key steps in the Risk Management process

The Risk Management process is divided into five steps, as shown in the following diagram:

The five steps of the Risk Management process

2.1. Risk Identification

2.1.1. Identify the risks

Risks typically fall into one or more of the following categories:

- **Risk of Ineffective Management**: Failure to achieve performance objectives (policy or control).
- **Risk of Inefficient Management**: Sub-optimal allocation of resources (human and/or financial) relative to achieved results (e.g., low productivity, disproportionate level of controls).
- **Risk of Uneconomical Management**: Resources not used for intended purposes, in due time, in appropriate quantity and quality, and/or at the best price (e.g., risk of over-expensive procurement).
- **Risk of Non-Protection of Staff or Safeguarding of Assets and Information**.
- **Risk of Non-Reliable Management and Financial Reporting**.
- **Risk of Non-Compliance**: Including legality and regularity of transactions with relevant legislation.

2.1.2 Considerations for Risk Identification

The EPPO should utilize the Commission's Risk Typology (**refer to Annex I**) to ensure comprehensive coverage of common risk aspects.

2.2. Risk Analysis

2.2.1 Clear Formulation of Risks

Before assessing a risk, it should be clarified:

- The **Impact on Activities/Objectives:** How would the risk affect the Sector/Unit's activities or objectives if it occurs?
- The **Root Cause:** What is the reason behind the risk, and what are the anticipated consequences?

2.2.2 Residual vs. Inherent Risk

Differentiation between inherent and residual risks should be ensured:

- **Inherent Risk**: Risks inherent to the EPPO's activities.
- **Residual Risk**: Assessed risk level after accounting for mitigating controls.

The risk assessment should be primarily performed at the residual risk level to avoid unnecessary administrative burden and complexity.

2.2.3 Cross-cutting risks

The Administrative Director and the Internal Control Officer are jointly responsible for the annual analysis of 'cross-cutting critical risks. The results of this evaluation should be discussed with the European Chief Prosecutor. This exercise is designed to facilitate Risk Management at the organizational level and ensure appropriate follow-up.

Critical risks are considered cross-cutting if they meet any of the following criteria:

- **Multi-Unit Impact**: The risk affects several units within the organization.
- **Collective Evaluation and Addressing**: The risk can be evaluated or addressed more effectively by a collaborative effort involving more than two units.
- **Potential for Cost-Effective Solution**: A cost-effective solution is not currently available but is deemed possible.
- **Lack of Management Structure**: A structure to manage the risk is not yet in place or has proven inadequate to address the risk concerned.

This approach will ensure that cross-cutting critical risks are identified, assessed, and managed effectively, leveraging the collective expertise and resources of multiple units within the organization.

Please refer to **Annex I** for a further analysis on risk inter-dependencies.

2.3. Risk Evaluation

2.3.1 Impact/Likelihood Approach

The EPPO should utilize the Impact/Likelihood approach to determine risk significance (a five-point scale from 1 (**very low impact, little likelihood**) to 5 (**very high impact, extremely likely**):

- **Impact**: Potential consequences if the risk materializes, quantitatively or qualitatively.
- **Likelihood**: Estimated probability of the risk occurring despite mitigating measures.

Please refer to **Annex I** for a detailed description of the risk assent criteria as well the EPPO risk heat map[5].

2.3.2 Prioritizing Critical Risks

A risk should be deemed "critical" and promptly reported if it meets any of the following criteria:

- **Jeopardizes Major Objectives**: The risk has the potential to significantly obstruct or prevent the achievement of the EPPO's primary goals.
- **Causes Serious Damage to Partners**: The risk could lead to substantial harm or disruption to the EPPO's partners, including Member States, companies, and citizens.
- **Results in Legal or Regulatory Infringement**: The risk could lead to the violation of laws and regulations, compromising the legal standing of the EPPO.
- **Causes Material Financial Loss**: The risk poses a significant threat of financial loss that could materially affect the EPPO's budget or financial stability.
- **Threatens Staff Safety**: The risk endangers the physical safety or well-being of the EPPO's employees.
- **Damages Image and Reputation**: The risk has the potential to seriously harm the EPPO's public image and reputation.

By systematically identifying and prioritizing these critical risks, the EPPO can take proactive measures to mitigate their impact and ensure continued operational integrity and public trust, except where mitigation is beyond management's scope due to budgetary constraints.

2.3.3 Documenting risks in a risk register

[5] A risk heat map is a visual tool that helps organizations assess and prioritize risks by plotting them based on two main factors: **likelihood** and **impact**. The purpose of a risk heat map is to highlight which risks need the most attention, allowing for more strategic decision-making.

To maintain focus and manageability, the most significant risks should be documented in a risk register. This provides a comprehensive record of risks and the measures taken to manage them. The EPPO's risk register provides an overview of the most significant risks faced by the organization. It includes key details about each risk, such as its nature, potential impact, likelihood, and current management status.

The risk register should include a minimum the following information:

- **Risk Description:** Detailed using the "cause - consequence" model. Record the risk level at its residual level (after considering the controls in place within the organization).
- **Inherent Risk Level** (Optional)**:** This is the risk level before controls are applied. Regular re-assessment of inherent risks is recommended to determine if existing mitigating controls are still effective, need enhancement, or can be reduced. However, inherent risk levels should not be the starting point for regular risk assessments to avoid unnecessary administrative burden with limited added value.
- **Risk type:** As per the risk typology described **in Annex I**.
- **Fraud Risk Classification:** Indicate if the risk could be related to or the result of fraudulent behaviour.
- **Proposed Risk Response:** Outline the recommended approach for managing the risk.
- **Action Plan:** Detail the specific actions to be taken, including the responsible owner and deadlines for completion.

By maintaining a detailed and regularly updated risk register, Sector/Units can ensure effective risk management practices and provide transparency and accountability in managing the organization's risks.

2.4. Risk Response

Each risk must have a defined response, documented in an action plan.

In principle, there are four possibilities or "risk responses". The identification of the most appropriate response should consider the impact and likelihood of occurrence of the risk. The response should control the risk cost-effectively, not "at all costs". The relevant risk responses are:

- **Avoid the Risk:** Modify the affected activities or objectives to eliminate the risk.
- **Transfer/Share the Risk:** Outsource the risk to third parties or use insurance.
- **Reduce the Risk:** Improve controls or take preventive actions to lower the risk. This is the most common risk response, especially for critical risks. Choosing this strategy implies:

  - Management defines and implements an action plan to address the risk.
  - Responsibility for different actions is allocated.
  - The impact/likelihood analysis is redefined to identify the residual risk in light of the action plan.
- **Accept the Risk:** Risk acceptance occurs when certain risks, despite applying mitigation measures, are acknowledged as manageable and are accepted at a specific level due to operational, resource, or strategic constraints. Management must recognize that not all risks can be entirely eliminated but should be reduced to a level deemed acceptable within the organization. The choice of the most appropriate strategy depends heavily on the risk level (the combination of impact and likelihood). While it is easier to accept a risk with low impact and likelihood, higher-impact and higher-likelihood risks should be mitigated where cost-effective to ensure that their impact does not threaten EPPO's objectives or operations.

Acceptable Risk Level ("Risk Tolerance"):

Risk Tolerance is the total impact of risk an organization is prepared to accept in the pursuit of its strategic objectives. The EPPO should define its acceptable risk levels for both quantifiable and unquantifiable risks. Critical risks exceed the acceptable risk level and require action unless the mitigation is beyond management's scope due to external factors.

Quantifiable Risks: For activities where risk exposure can be quantified, management should assess whether this level is acceptable. This assessment should be carried out at the activity level. A specific assessment of the financial impact linked to an action needs to be conducted. This assessment should consider the cost-effectiveness of further controls—additional controls are warranted if each additional Euro spent reduces the error by more than one Euro.

Unquantifiable Risks: For risks where financial exposure cannot be quantified, management must define exposure using appropriate measures such as reputational impact or regulatory compliance. A "zero tolerance" approach may be adopted for certain unquantifiable risk areas, such as staff security.

Establishing and Implementing Action Plans:

To establish effective action plans, the root causes of risks and their consequences must be fully analysed and understood. The level of detail required will vary according to the impact and likelihood of the risk. As a minimum, action plans should include:

- A description of the risks and the actions to be taken.
- The owners of these actions (responsible for implementing the defined measures).
- Target dates and milestones.

2.5. Monitoring & Reporting

Monitoring the implementation of action plans is fundamental to ensure they continue to be effective and relevant.

- For example, identified risks may evolve and new risks may emerge, potentially making current actions less effective or inadequate. Therefore, regular monitoring is essential. This task should fall to management, with oversight by the Internal Control Officer for the most significant risks.

Reporting on the implementation of action plans is mandatory.

- This reporting should be carried out in the Annual Activity Report. As the report is public and should not contain sensitive information, detailing specific individual risks should be avoided. Instead, it should provide general information about key activities and how overall risk levels have been managed. For risks that materialize during the reporting year, a more detailed disclosure is required, including an assessment of whether a reservation to the Authorising Officer's Declaration of Assurance is necessary.

3. Risk Management in practice

3.1. Planning and organisation

3.1.1. Skills and awareness

Knowledge as a Critical Success Factor:

- Managers and staff involved in the Risk Management exercise should have sufficient knowledge of its purpose, main concepts, and bases for assessing impact and likelihood. They should understand the relevance of risk assessment to the work program and the achievement of objectives to avoid perceiving Risk Management as a purely administrative burden with little value.

Risk Management Training (EULearn):

- Risk Management courses are regularly available and should be carried out by the relevant managerial and non-managerial staff of the EPPO.

Risk Management Seminars:

- Risk Management seminars can effectively raise awareness among management and staff and therefore should be organised within the EPPO according to the relevant staff availability. The Internal Control Officer can facilitate general or targeted risk assessment exercises during these seminars.

Information Resources:

- A range of useful information regarding Risk Management is available on BudgWeb and should be systematically taken into account by the relevant staff of the EPPO.

3.1.2. Coordination

Flexibility:

- The Risk Management exercise should be internally coordinated. The annual exercise should be integrated within the Single Programming Document process, while also maintaining its continuous nature to allow for responses to a changing risk environment. The Internal Control Officer should serve as the center of competence, offering technical advice, facilitating the Risk Management process, and contributing to reporting. The Internal Control Officer should also acts as a contact point for matters concerning Internal Control and Risk Management.

Documenting Roles and Responsibilities:

- To ensure clarity and promote understanding within the EPPO, the main roles and responsibilities related to the organization and coordination of the Risk Management exercise should be documented.

3.1.3. Communication to participants

- **Involve Management**: Effective Risk Management requires strong involvement from management. Workshops, seminars, and similar events should be organized according to the staff's needs. The Risk Management exercise should be proposed by the Administrative Director to the European Chief Prosecutor for agreement.
- **Presentations**: Presentations or workshops at the Sector/Unit level to explain the purpose, basic concepts, and practical arrangements to participants should be organised according to the staff's needs. In-person presentations or management meetings should be privileged as they are more effective than emails or websites for communication.

3.1.4. Scope and approach

- **Management Steer:** The Administrative Director should lead the Risk Management exercise. This includes defining the annual coverage and determining the necessity of additional risk reviews for processes, projects, or systems throughout the year.
- **Focus on Higher-Risk Activities:** The exercise should prioritize areas representing the highest risks.
- **High-Level Review:** A high-level review can identify activities or areas that may require a more detailed, targeted review.
- **Targeted Review:** This approach typically excludes "low-risk areas"—stable and well-known activities—from the scope. Alternatively, the review can be structured around "risk themes" defined.
- **Bottom-Up Perspective:**A "bottom-up" approach might also be adopted. This involves an extensive review of all main activities and objectives down to the Unit level.
- **A Balanced Approach:** A balanced approach can be tailored to the EPPO's needs, combining elements of both top-down and bottom-up methodologies as appropriate.

3.1.5. Stating outputs and activities related to objectives

Potential threats that could impact the achievement of the EPPO's objectives should be identified, and corresponding mitigating actions should be defined as part of a critical risk assessment exercise.

- **Activities or Objectives/Outputs:** According to Risk Management principles, "objectives" or outputs (what should be achieved?) are generally preferred over "activities" (description of foreseen actions) as the basis for risk identification. However, in practice, since activities are the means to achieve objectives/outputs and indicators measure progress towards achieving the objectives, any of these elements (objectives, activities, outputs, indicators) can be used as deemed appropriate by the Administrative Director and/or the Heads of Units.
- **Define Objectives, Related Actions, and Outputs Clearly**: It is crucial that the objectives, activities, outputs, and indicators used for risk identification are clearly defined. If they are unclear or vague, the risks identified will likely also be unclear and vague. Objectives, activities, outputs, and indicators may be reformulated or regrouped for the purposes of the Risk Management exercise. Where possible, objectives should be established according to the SMART criteria (Specific, Measurable, Approved, Realistic, and Timed).

3.2. Risk identification and assessment

3.2.1. Risk identification

- **Risk Identification Methodology:** Risk identification should involve a combination of desk reviews, questionnaires, interviews, and brainstorming sessions (please refer to **Annex I** for further details on the methodology).
- **Multi-Annual Planning Environment:** In a multi-annual planning context, risks associated with ongoing actions should be carried forward automatically from one year to the next. However, these risks must be re-assessed for each upcoming programming exercise to ensure their relevance and accuracy.

3.2.2. The role of external partners in the risk identification process

External partners' views, including those of institutional stakeholders, contractors, beneficiaries, and EU citizens, should be considered in the risk identification process where relevant. Their opinions can be gathered through various measures, such as:

- **Surveys:** Conduct surveys on topics like service quality, payment deadlines, and proposed new legislation.
- **Review of Complaints:** Analyse recent complaints submitted to the Commission or Ombudsman.
- **Reports and Resolutions:** Utilize insights from European Court of Auditors' reports and Discharge resolutions.
- **Dialogue with National Administrations:** Engage in discussions with national administrations of Member States.
- This list is not exhaustive. Care should be taken to ensure that the views of external partners are relevant to the EPPO's objectives before incorporating them into the risk assessment.

3.2.3. Critical risks

For the **critical risks**, the following should be taken onto account:

- **Mandatory Reporting:** Critical risks must be reported in the Annual Activity Report (AAR) and the Single Programming Document. The residual risk level, rather than the inherent risk level, should be considered when defining criticality.
- **Overall EPPO Perspective:** The identification of critical risks should be carried out from an overall EPPO perspective to ensure a balanced and comprehensive assessment.

- **Formal Validation of Risks:** The European Chief Prosecutor (ECP) validates critical risks as well as the respective action plans based on a proposal submitted by the Administrative Director.
- **Sensitive Risks:** Certain critical risks may be sensitive, such as those related to security issues or third parties. Care should be taken in formulating these risks and referencing them in the AAR to avoid causing harm to the EPPO or its partners.
- **Linking Critical Risks and the AAR:** A critical risk can become a reservation in the subsequent AAR if not adequately managed. Similarly, a Risk Management action plan must be developed for reservations noted in the AAR of the previous year (year n-1). Reservations from year n-1 should also be considered when assessing the criticality of risks in the current year (year n).

3.2.4. Cross-cutting risks

For critical risks that are potentially cross-cutting, peer reviews should be organized with the concerned Sectors/Units to gather detailed information, estimate the risk level, and assess the most appropriate organizational level for managing the risk. The process should involve:

- **Gathering Detailed Information:** Engage relevant units to collect comprehensive data about the risk.
- **Estimating the Risk Level:** Evaluate the severity and impact of the risk through collaborative assessment.
- **Assessing Management Level:** Determine the most suitable organizational level for managing the risk.
- **Assigning a Lead Unit (Chef de File):** Designate a lead unit responsible for managing the risk.
- **Establishing an Action Plan:** Develop a detailed action plan to address the risk.

The designated Lead Unit is responsible for ensuring the implementation and delivery of the actions decided upon during the peer review process.

3.3. Reporting and action plans

3.3.1. Special case - risks outside management's control

- **Risks Outside the Control of the EPPO**: These risks predominantly fall under Category 1 -"Risks Related to the External Environment"- (Annex I). For most of these risks, the primary response should be to "Accept" them, though some measures to mitigate their impact may be feasible. Given the lack of direct control over these risks,

they should be monitored more frequently than annually—ideally on a quarterly basis to:

- **Verify and Confirm Risk Categorization**: Regularly reassess whether the risks remain classified as critical, important, or low risk.
- **Verify Control Status**: Check if the risks are still outside management control and identify any additional measures that might be taken to mitigate their impact.

Examples of Risks Outside Management's Control:

- **Sudden Crises**: Political instability, economic downturns, natural disasters, and health crises.
- **Stakeholder Engagement**: Failure of Member States, authorities, or stakeholders to engage effectively in achieving shared objectives.
- **External Contractors**: Risks of delays in implementing crucial IT systems due to the underperformance of external contractors.

3.3.2. Re-assessment and Continuous Updating of Risk Registers

Although risks should be assessed at their residual level as a standard practice, the most significant inherent risks should be periodically re-assessed. This exercise contributes to determine whether the existing mitigating controls are still effective, need enhancement, or can be reduced. However, inherent risk levels should not be used as the starting point for routine risk assessment exercises, as this approach can significantly increase administrative burden without providing substantial added value.

Risk registers should be updated to reflect the implementation of action plans and the emergence of new risks. This updating process should occur continuously, meaning updates should be made as soon as relevant changes occur. Responsible managers should handle these updates, with oversight and monitoring provided by the Internal Control Officer.

3.3.3. Action plans

An action plan should describe the detailed and concrete measures to be taken to implement the risk response strategies. It should specify the actions required to address each identified risk, assigns responsibilities, sets deadlines, and includes metrics for evaluating the effectiveness of the response.

Developing clear and comprehensive action plans is crucial for effective risk management. These plans should clearly allocate responsibilities and set timelines for actions to ensure that risks are addressed according to management's directives. Action plans serve as the benchmark for tracking progress and are especially important for long-term actions, such as major projects.

While there are no mandatory formats for action plans, they should clearly identify:

- **Risk Description**: The specific risk being addressed.
- **Action Plan Goals**: Objectives that the plan aims to achieve.
- **Target Dates and Milestones**: Key deadlines and progress markers.
- **Action Owners**: Individuals responsible for each action.
- **Specific Actions**: Detailed steps to be taken.
- **Resources Needed**: Required resources and their allocation.
- **Monitoring/Reporting Arrangements**: Procedures for tracking progress and reporting.

Regular monitoring of action plan implementation serves two main purposes:

1. **Progress Tracking**: Ensuring that actions are progressing according to plan.
2. **Relevance Checking**: Confirming that the planned actions remain relevant as risks evolve and new risks emerge. Action plans must be updated as needed.

Responsible managers should oversee the implementation of action plans. The Internal Control Officer should centrally monitor the risk register to ensure comprehensive oversight.

Monitoring should not be restricted to critical risks alone but should also encompass other significant risks within the EPPO, such as the top 10-15 risks. Insufficient monitoring of these risks can lead to delayed management responses if their importance increases in the future.

The results and conclusions from monitoring should be documented and reported to the relevant management levels. The Administrative Director and the ECP should be regularly informed about the evolution of critical risks.

3.3.4. Contingency plans for accepted critical risks

EPPO may occasionally decide to accept a risk of critical nature, even after mitigating measures have been considered. This decision may occur in two scenarios:

- **External Risks**: The risk is beyond the EPPO's control (e.g., economic crises, pandemic).

- **Deliberate Decision**: EPPO makes a conscious choice to accept the risk.

In both scenarios, the EPPO must establish a follow-up (contingency) plan outlining the actions to be taken if the risk materializes. This contingency plan should be designed to manage and mitigate the impact of the risk. It should include:

- **Decision-Making Responsibility**: The persons responsible for making decisions related to the risk and its contingency plan (the Administrative Director and the ECP).
- **Actions and Ownership**: Specific actions to be taken if the risk materializes, including responsible owners for each action.
- **Involvement of Other Sectors/Units**: Identification of other units involved in implementing the contingency plan.

The existence of a contingency plan for accepted critical risks should be noted in the risk register.

3.4. Specific risk reviews

Besides identifying risks during the programming phase, detailed risk reviews of specific key processes, projects, or systems could also take place. These reviews should be scheduled at appropriate times based on the planning and execution cycles of the activity in question.

When performing specific risk reviews, the core Risk Management principles should be applied:

- **Defining Activities and Objectives**: Clearly identify what the process, project, or system aims to achieve.
- **Identifying and Assessing Risks**: Use the impact/likelihood method to evaluate risks.
- **Deciding on Risk Management**: Determine how to address the identified risks, considering what levels of risk are deemed acceptable.
- **Action Plans**: Develop and implement action plans to manage the risks.
- **Follow-Up**: Monitor the implementation of action plans to ensure they are carried out effectively.

Project managers or relevant line managers oversee and coordinate specific risk reviews. They are supported by appropriate staff, and the Internal Control Officer may assist if necessary. External specialists should also be involved if required.

Specific risk reviews generally have a more detailed scope compared to the annual Risk Management exercise. Depending on the complexity and scale of the process, project, or system, the review duration can range from a few days to several weeks.

The Internal Control Officer should be informed of all specific risk reviews to ensure alignment with the overall EPPO risk management framework.

To prepare for a risk review, it is recommended to graphically represent the process, project, or system using flow charts. This visual representation aids in defining the review scope and serves as a basis for risk identification. The scope can include the entire process or specific phases as needed.

ANNEX I

A. Risk Typology

The EPPO's risk typology is mandatory and all risks are classified according to the main risk groups. Such an approach helps ensure that the most common risk aspects are covered and provides for a consistent basis for analysis across the organisation. The typology is primarily designed to facilitate the identification of risks. However, it may also be used for the consolidation of risks at a central level (categorising the risks by cause or by consequence).

Example of risks based on the risk typology

Risk typology		
External	1. Risks related to the external environment (outside EPPO)	- Macro-environmental risks (geo-political, economic, natural disasters etc.) - Political decisions and priorities outside the EPPO (Parliament, Council, Commission, Member States etc.) - External partners (agencies, outsourcing, consultants, media, etc.)
Internal	2. Risks related to planning, processes and systems	- Operational processes (process design and description) - Financial processes and budget allocation - IT and other support systems
	3. Risks related to people and the organisation	- Human resources (staffing, competencies, collaboration) - Ethics and organisational behaviour ("tone at the top", fraud, conflict of interests etc.) - Internal organisation (governance, roles and responsibilities, delegation, etc.) - Security of staff, building and equipment

	4. Risks related to legality and regularity aspects	- Clarity, adequacy and coherence of applicable laws, regulations and rules - Other potential issues related to legality and regularity
	5. Risks related to communication and information	- Communication methods and channels - Quality and timeliness of information

Methodologies for risk identification

Method	Advantages (+)/Disadvantages (-)
Desk Reviews: A desk review is a structured review of audit reports, results of ex-ante/ex-post controls, exception reports or other reports or studies that provide information about possible risks. The desk-review is usually carried out or coordinated by the Internal Control Officer. Ideally, the results and conclusions of the desk review should be documented.	+ Utilizes existing information, making it cost-effective. + Provides a comprehensive overview of documented risks and issues. + Allows for the identification of risks based on historical data and trends. - May not capture current or emerging risks. - Relies on the quality and completeness of existing documentation. - May miss context-specific risks not documented in the reviewed materials.
Questionnaires: All persons participating in the risk identification exercise are invited to complete a Risk Management questionnaire (pre-filled or blank).	+ Can reach a wide audience, providing diverse perspectives. + Allows for the collection of specific and standardized information. + Useful for identifying common concerns and risks across different areas. - Responses may lack depth and context. - Risk of low response rates or incomplete responses.

	- May not fully capture complex or nuanced risks.
Interviews: The Internal Control Officer organises bilateral interviews with relevant managers and key staff in order to get their view on possible risks related to their activities and objectives.	+ Provides detailed and in-depth information. + Allows for the exploration of complex and context-specific risks. + Facilitates the understanding of stakeholder concerns and perspectives. - Time-consuming and resource-intensive. - Potential for interviewer bias. - May require skilled interviewers to obtain valuable insights.
Brainstorming/Workshops: The Internal Control Officer organises brainstorming sessions with relevant managers and staff.	+ Encourages creative thinking and diverse ideas. + Facilitates collaboration and knowledge sharing. + Can quickly generate a large number of potential risks. - May result in a broad list of risks without prioritization. - Risk of dominant participants influencing the outcome. - Requires effective facilitation to be productive.

Additional Considerations for Risk Identification

- **"Fresh Eyes":** To prevent successive Risk Management exercises from becoming routine and detecting few new risks, it may be beneficial to change the risk identification methodology each year and involve different staff members if feasible. This approach can bring new perspectives and insights, enhancing the identification process.
- **Use of Common Risk Typology:** Various internal and external risks can impact compliance with rules and regulations, operational effectiveness, or the safeguarding of assets and information. The mandatory Commission risk typology (**see Annex I**)

ensures that the most common risk aspects are covered and that risk categories remain consistent across all units. This common typology serves three main purposes:

- **Communication:** Establishes a common Risk Management language.
- **Risk Identification:** Assists management in considering all risk aspects and potential areas during the identification phase.
- **Analysis and Reporting:** Aids in the analysis, consolidation, and reporting of risks.
- **Formulating Risks Clearly:** For effective risk assessment, it is crucial to clearly define and formulate risks. This involves identifying the main causes (underlying problems) and potential consequences (impact on activities or objectives) if the risks materialize.
- **Ensuring Completeness of the Exercise Scope, Including Fraud Risks:** A comprehensive risk assessment exercise must consider all types of potential risks. Managers often focus on operational risks encountered in daily management while overlooking peripheral risks. To address this, ensure that the sample of contributors is representative of all professional functions and encompasses all domains, areas, and processes managed by the organization. Additionally, compliance risks should be considered not only from an error perspective but also for potential fraud implications, requiring a specific approach within the overall risk exercise. The results of the Fraud Risk Assessment (FRA), conducted as part of the Anti-Fraud strategy update, should be cross-referenced with the annual risk exercise to ensure completeness.

B. Risk assessment criteria

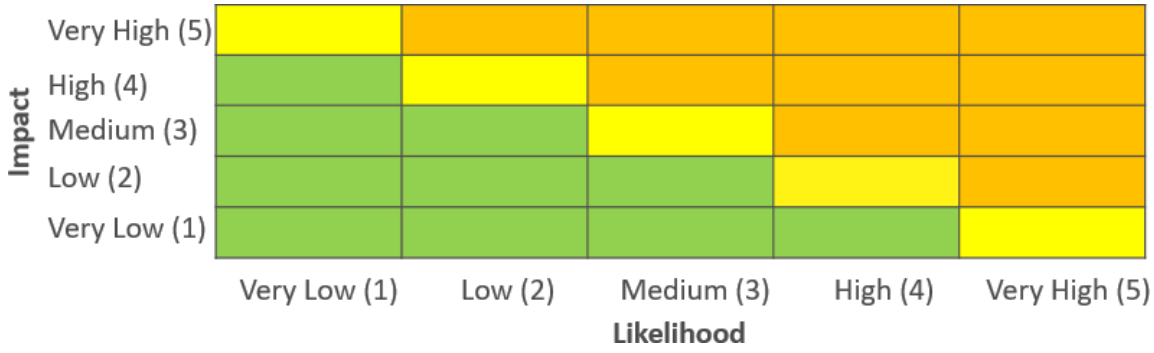
Likelihood	Description	Probability
1	Very Low: uncertain event (or set of events) is (are) extremely unlikely to occur	< 5%
2	Low: uncertain event (or set of events) is (are) unlikely to occur	5-15%
3	Moderate: uncertain event (or set of events) is (are) may occur	15-30%
4	High: uncertain event (or set of events) is (are) likely to occur	30-70%
5	Very High: uncertain event (or set of events) is (are) most likely to occur	>70%

Impact	Reputational Impact Scope	Possible impact on the achievement of EPPO Mission	Possible impact on the achievement of EPPO objectives (as per SPD)	Financial Impact
1	Very Low: Internal reputational impact within EPPO and its College	Very Low: The achievement of EPPO mission is not impacted	Very Low: Inefficiencies with regards to the achievement of the objective	Very Low: Financial impact up to €50k

Impact	Reputational Impact Scope	Possible impact on the achievement of EPPO Mission	Possible impact on the achievement of EPPO objectives (as per SPD)	Financial Impact
2	Low: An EPPO act is object of a formal enquiry by a supervisory body (e.g. EU Ombudsman, EDPS,...) or adverse public reputational impact limited to one member State through non-major public communication chanel	Low: The achievement of EPPO mission is unlikely to be impacted	Low: The achievement of the objective is delayed	Low: Financial impact between €50k-€100k
3	Moderate: An EPPO act is object of a formal enquiry by an institution (e.g. ECA, Council, European Parliament, ...); a negative finding is made by a supervisory body (e.g. EU Ombudsman, EDPS,...) identifying weaknesses not of a nature to put into question the capaciy of EPPO to perform its mission and / or to operate within standards expected from EU public service; adverse public reporting by major communication chanel(s) or multiple minor communication chanel(s)	Moderate: The achievement of EPPO mission might be impacted (50% or less)	Moderate: The achievement of the objective is threaten	Moderate: Financial impact between €100k-€200k
4	High: A formal inquiry by an institution (e.g. ECA, Council, European Parliament, ...) concludes on weaknesses not of a nature to put into question the capaciy of EPPO to	High: The achievement of EPPO mission is possible to be impacted (50% or more)	High: The achievement of the objective is endangered	High: Financial impact between €200k-€300k

Impact	Reputational Impact Scope	Possible impact on the achievement of EPPO Mission	Possible impact on the achievement of EPPO objectives (as per SPD)	Financial Impact
	perform its mission and / or to operate within standards expected from EU public service			
5	Very High: Negative headlines in major communication channels (e.g. press, social media, …) and negative findings as a result of a formal inquiry by an institution (e.g. ECA, Council, European Parliament, ...) putting in doubt the capaciy of EPPO to perform its mission and / or to operate within standards expected from EU public service	Very High: The achievement of EPPO mission is in danger	Very High: The objective will not be achieved	Very High: Financial impact close to materiality (€300k and above)

C. EPPO risk heat map

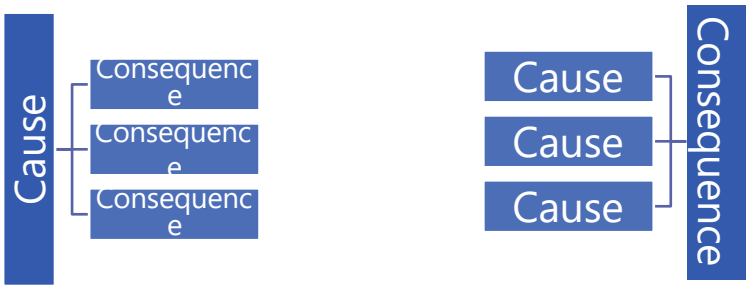


D. Risk inter-dependencies

Cause ➔ Consequence

When identifying potential events that might cause risks, it should be define all the possible risks that might result from a single cause. Conversely, a risk may materialize only if multiple causative events occur simultaneously. Both scenarios are illustrated in the following diagrams:

- Single Cause, Multiple Consequences: One cause can lead to several risks.
- Multiple Causes, Single Consequence: Several events must occur together to materialize a risk.



When assessing the most significant risks, it is crucial to identify any potential consequences on other EPPO activities. Consider the following example:

- **Example:** If Risk A is a potential cause of Risk B and the likelihood of Risk A occurring is low, it is probable that the likelihood of Risk B occurring is also low.

This approach helps in understanding how risks are interconnected and ensures that potential impacts on other activities are adequately considered in the risk management process.

Risk response

Risk responses can affect the likelihood or impact of other risks. These inter-dependencies should be considered when defining and implementing risk responses. For example:

- **Acceptance of Risk:** Accepting Risk A may increase the likelihood of Risk B. For instance, if a unit accepts the risk of a high workload, it might lead to significant staff turnover in the future. Management may have ranked this risk as 'low likelihood.' However, if it materializes, the relationship with stakeholders, such as a contractor developing an IT system, could deteriorate. This could impact the contractor's output quality and hinder the EPPO's objective of implementing the IT system on time.
- **Mitigation of Risk:** Mitigating Risk A may inadvertently increase the probability of Risk B occurring. For example, implementing a new IT system to combat fraud could lead to a higher workload for staff. This additional workload may result in staff dissatisfaction and potential turnover, affecting the EPPO's operations.

Risk inter-dependencies should be identified at each stage of the risk management process. The examples provided illustrate potential scenarios, emphasizing the need for careful consideration and regular follow-up to ensure that inter-dependencies between risks are managed effectively.

E. Glossary of Key Risk Management Terms

- **Acceptable Risk Level ("Risk Tolerance"):** The amount of risk that an organization is prepared to accept in pursuit of its objectives.
- **Action Owner:** The individual responsible for implementing actions specified in a risk response plan.
- **Contingency Plan:** A predefined set of actions to manage and mitigate the impact of accepted critical risks if they materialize.
- **Fraud Risk Classification:** Categorization of risks associated with or resulting from fraudulent activities.
- **Inherent Risk:** The level of risk that exists before applying any controls or mitigating measures.
- **Residual Risk:** The remaining level of risk after implementing mitigating actions.
- Risk Interdependencies: Relationships between risks where one risk can affect the likelihood or impact of another.
- **Risk Register:** A document recording identified risks, their assessments, and associated management strategies.
- **Risk Response:** The strategies for addressing identified risks, such as avoiding, mitigating, transferring, or accepting them.
- **Specific Risk Review:** Detailed evaluation of particular processes, projects, or systems to identify and address risks.