DECISION OF THE COLLEGE OF THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE OF 12 MAY 2021

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

The College of the European Public Prosecutor's Office (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, 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."

(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

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

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 DECIDED AS FOLLOWS:

Article 1

Adoption of EPPO's Risk Management Policy

EPPO's risk management policy, as set out in the Annex to this decision, is hereby adopted.

Article 2

Entry into force

This decision shall enter into force on the date of its adoption by the College.

Done at Luxembourg on 12 May 2021.

On behalf of the College,

Laura Codruța KÖVESI
European Chief Prosecutor

EUROPEAN PUBLIC PROSECUTORS OFFICE

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

1. Definitions and concepts

1.1. What is a risk?

At the European Public Prosecutor's Office ('EPPO'), a risk is defined as "Any event or issue that could occur and adversely impact the achievement of the EPPO's political, strategic and operational objectives. Lost opportunities are also considered as risks".

Hence, risks relate to the non-achievement of objectives. Risks can be associated with the EPPO's specific and organisational management objectives or with the implicit objectives of protecting staff and safeguarding assets and information.

Note that "lost opportunities" are also considered as risks. This type of risk relates to the development and modernisation of the organisation and its activities, i.e. the adaptation to new circumstances and expectations. If the organisation is not capable of cutting across traditional boundaries and implementing change, the risk that it becomes less effective, less relevant and eventually obsolete increases.

1.2. What is Risk Management?

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

Practically, Risk Management is about identifying and carefully assessing potential problems that could affect the execution of the organisation's activities and the achievement of its objectives. The risks are then prioritized according to their relative significance (usually measured in terms of potential financial and other impact), and actions taken to reduce them to a level judged acceptable by management. Hence, the aim is not to avoid risks at all costs. Reducing the risk to zero is, in most cases, practically unfeasible and rarely cost effective. Furthermore, a certain degree of risk-acceptance is necessary to keep the organisation dynamic.

A common misunderstanding is that Risk Management (and Internal Control in general) only concerns financial procedures. This is not the case. Risk Management embraces all domains and management aspects, such as strategic decision-making and activity planning, operational effectiveness and efficiency, protection of assets and information, business continuity or staff management.

Largely, Risk Management is common sense: every manager naturally reflects on and manages potential problems that could affect his/her activities and objectives. However, the

approach set out in this document aims at making Risk Management a continuous, systematic and structured exercise.

1.3. How does Risk Management add value?

Risk Management is not an "optional add-on" to an organisation's activities, but should be an integral part of the management process at all levels which adds value, increasing the likelihood of achieving objectives efficiently and effectively. Risk management should not be a one-off or annual bureaucratic exercise: the level of resources devoted to it, and the level of documentation will 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. When integrated into "normal business", Risk Management can be expected to have the following benefits:

- **Generally**: effective Risk Management can strengthen the communication process, support strategic and operational management decisions, trigger new ideas and solutions, and provide useful information for establishing appropriate control environment and strategies (less control in certain areas, better control in others).
- **At management level**: a structured and consistent management approach facilitates the coordination, analysis and management of risks at organisation level. It is also necessary for the effective management of cross-cutting risks affecting several units.
- **At unit level:** a systematic and continuous Risk Management process, involving all relevant staff, can help the manager carry out his/her management duties, i.e.:
    - achieve the unit's objectives effectively and efficiently;
    - ensure that activities and transactions under his/her responsibility comply with applicable law, rules and regulations;
    - ensure that effective measures to prevent and detect fraud are in place and due follow-up is given to instances of fraud;
    - manage and protect staff, assets and information;
    - compile accurate, relevant and timely reporting (financial and other reports).

1.4. Who should perform Risk Management?

Risk Management is part of the management of an activity and all those performing each activity should also assess and manage the risks associated to it. Within this overall framework, different actors intervene at different hierarchical levels:

- The **European Chief Prosecutor** is ultimately responsible for the management of the EPPO's activities and achievement of objectives and must ensure that the EPPO's critical risks are known and appropriately managed. In his/her quality of authorising officer, the Administrative Director shall put in place the organisational structure and the internal control systems suited to the performance of his/her 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 "setting the tone" for Risk Management, sponsoring Risk

Management exercises, assigning responsibilities and reaching a view on the treatment of critical risks.

- **Managers and members of staff** as the experts are responsible for managing risks related to their main activities and objectives;
- The **Internal Control Officer** supports managers in setting up a coherent and effective Risk Management process in their unit. The role involves facilitation, support and monitoring rather than directly managing risks;
- The **Internal Audit Capability** (IAC) performs independent regular assessments and makes recommendations for improving the effectiveness of risk management, control and governance processes. The mission and objectives of the IAC are presented in detail in the Internal Audit Charter;
- The **College** is kept informed of critical risks affecting the EPPO, as required by the Internal Control Principles.

1.5. Risk Management and the Internal Control Principles

Risk Management is part of effective internal control. Whereas the 17 internal control principles (ICPs) constitute the basic management principles, Risk Management facilitates the establishment of unit-specific internal control environments and strategies focussing on the activities and domains representing the highest risks. It should be borne in mind that risks may be in financial or non-financial areas and that financial aspects do not necessarily pose the greatest threat to the organisation.

1.6. Risk Management

To be effective, Risk Management must be part of everyday management (with the level of action dependent on the level of risk involved). To ensure readiness to react to new or changed risks and threats, Risk Management is a continuous exercise. Therefore, Heads of Unit are strongly encouraged to assess the risks whenever they identify the need to do so and notably where there are major changes to policies and/or procedures. The factors, which might justify a reassessment of risks, are:

- reorganisation of the unit;
- staff changes in crucial positions (particularly key management and specialist staff);
- external events e.g. financial crisis, threat of pandemic, natural disaster;
- new legislation;
- failure of Risk Management as regards critical risks.

Risk Management should also be a regular point on the agenda of management meetings, and where appropriate unit meetings. This will enable management to monitor how risks are being managed and to react to changes in exposure where appropriate.

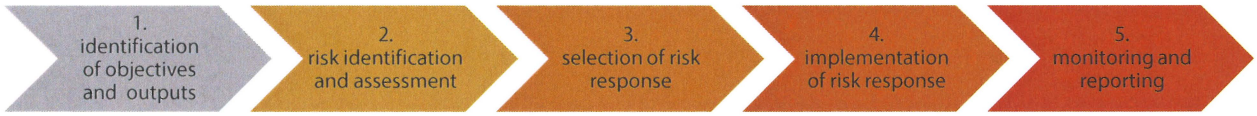
Although Risk Management is a continuous exercise, and regular monitoring may take the form of an informal exercise, formalisation is mandatory only once per year. Heads of Unit are

required to submit their list of critical risks as part of the Single Programming Document exercise. However, Heads of Unit should notify on an ad-hoc basis when they identify additional critical risks, in the course of the year.

2. The key steps in the Risk Management process

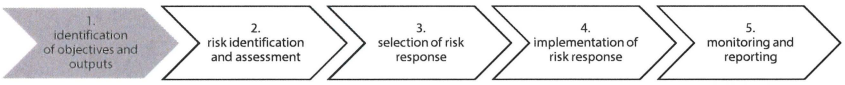
The Risk Management process is divided into five steps, as shown in the following diagram:

The five steps of the Risk Management process



2.1 Stating objectives and outputs to deliver

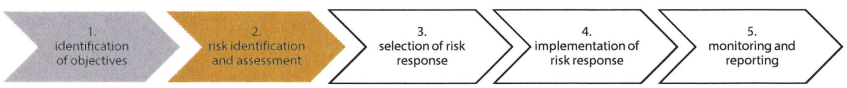
What is the purpose of the unit's activities? What should be achieved (outputs) in the year ahead?



- Clearly stating objectives and identifying the corresponding outputs for the year provides a firm basis for Risk Management.
- Deciding what to cover: the Risk Management exercise does not have to cover all activities and objectives in depth. Focus should be on the major activities and those areas considered the most risky, for example activities, processes or systems that are new or form a significant part of the work programme, have undergone significant change or have not been reviewed for a long period.

2.2. Identifying and assessing the risks

What can go wrong? How bad would it be?



2.2.1. Identify the risks

Risks typically fall into at least one of the following categories:

a) risk of ineffective management: non-achievement of political, strategic or operational performance objectives (policy or control);

b) risk of inefficient management: sub-optimal relation between invested (human and/or financial) resources and achieved results (e.g. low productivity, disproportionate level of controls);

c) 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);

d) risk of not protecting staff or safeguarding assets and information;

e) risk of non-reliable management and financial reporting;

f) risk of non-compliance (e.g. legality and regularity of transactions, legislation);

g) lost opportunity.

- *Taking into account all aspects when identifying risks*: risk management refers to all the domains and management aspects and covers many types of risks, both internal and external, depending on the specific nature of activities. The EPPO applies the Commission's Risk Typology (see **Annex I**) which sorts these risks into groups and it should be used to ensure that the most common risk aspects are covered. When assessing risks, managers naturally tend to focus on the operational risks, which they confront in day-to-day management. Therefore, the risk assessment exercise must be designed to ensure that all aspects and risks are adequately covered.
- *Formulating the risks clearly*: before assessing a risk, it must be clearly explained: (1) How would it impact the unit's activities/objectives if it occurred? (2) What is the reason (root cause) for the risk? What are the foreseen consequences?
- *Using the Impact/Likelihood-approach to determine the significance of the risks (risk level)*: It is vital to determine the significance of a risk to ensure that the reaction to the risk is proportionate with the exposure implied by that risk. The impact is the potential consequence should the risk materialise. It can be both quantitative and qualitative in nature. The likelihood is the estimated probability that the risk will materialise even after taking account of the mitigating measures put in place (the residual risk). The assessment of impact and likelihood is often based on subjective judgments, but can in some cases be supported by objective data, if available. A five-point scale must be used for this assessment, ranging from 1 (very low impact, little likelihood) to 5 (very high impact, extremely likely to happen).
- *Residual vs. inherent risk:* Management should be aware that residual (not inherent) risks are subject to risk assessment. Inherent ('gross') risk is the risk related to the very nature of the organisation's activities. Residual risk is the assessed level of ('net') risk remaining when taking into account those controls already in place to mitigate the inherent risk. The assessment of the risk impact/likelihood must therefore take account of all controls put in place or planned.

While it is a rule that risks are assessed always at their residual level, it is recommended to regularly re-assess the most apparent inherent risks, in order to conclude whether related

mitigating controls are still effective/should be enhanced/reduced. However, a regular risk assessment exercise should not take inherent risk level as a starting point for assessment, as this would significantly increase administrative burden and complexity (discussing 'theoretical risk' levels can be quite 'abstract') with little added value.

2.2.2. Prioritise the risks (identify "critical" risks)

- *Determining if any risks are "critical"*. A risk should be considered "critical" and reported if it can:
  a) jeopardise the realisation of major policy objectives;
  b) cause serious damage to the EPPO's partners (Member States, companies, citizens, etc.);
  c) result in critical intervention at political level (Parliament, Council, Commission) regarding the EPPO's performance;
  d) result in the infringement of laws and regulations;
  e) result in material financial loss;
  f) put the safety of the EPPO's staff at risk; or
  g) in any way seriously damage the EPPO's image and reputation.

2.2.3. Cross-cutting risks

The Administrative Director and the Internal Control Officer are jointly responsible for the annual 'cross-cutting critical risks' analysis. This exercise is designed to facilitate risk management at organisation level in order to ensure the appropriate follow-up.

Critical risks are considered cross-cutting if:

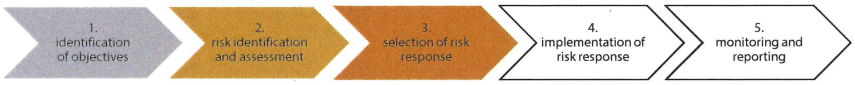
- they affect several units;
- they can be evaluated or addressed more effectively by a group (more than two) of units;
- a cost-effective solution is not (yet) available, but is possible;
- a structure to manage the risk is not yet in place or has not been able to address the risk concerned.

2.2.4. Documenting risks in a risk register

- *Documenting the most significant risks in a risk register*: to make the exercise focussed and manageable, the most significant risks must be documented in a risk register to provide a record of risks and the measures taken to manage them. It is required that each unit keeps a regularly updated risk register containing the most significant risks. The minimum mandatory format of the risk register is presented in **Annex II**.

2.3. Deciding how to deal with the identified risks ("risk response")

How will the EPPO manage identified risks? To what extent can the risks be accepted?



Each risk must have a defined response, which should be documented in an action plan at the appropriate level where the residual risk is judged to be lower, and centrally where the risk is considered sufficiently important by management.

- *Determining how to deal with the identified risks:* in principle, there are four possibilities, or "risk responses". The identification of the most appropriate response should take into account the impact and likelihood of occurrence of the risk (that is the response should control the risk cost-effectively and not "at all costs"). The relevant risk responses are:

  1) **Avoid** the risks (for example by modifying the affected activities or objectives);

  2) **Transfer** them to/share them with third parties (for example by outsourcing or using an insurance company);

  3) **Reduce** the risks (for example by improving controls or taking other relevant action, notably of preventive nature) - most common risk response, especially for critical risks. Choosing this strategy implies that Management defines and implements an action plan to address the risk, allocates responsibility for the different actions and redefines the impact/likelihood analysis to identify the residual risk in the light of the action plan;

  4) **Accept** the risk - the strategy usually applicable to risks with low impact and low likelihood.

Management should bear in mind that the choice of the most appropriate strategy (risk response) depends heavily on the risk level (the combination of impact and likelihood). Whereas it is quite easy to accept a risk with low impact and low likelihood, a risk with high impact and high likelihood should probably be the subject of enhanced mitigating measures where these are cost effective.

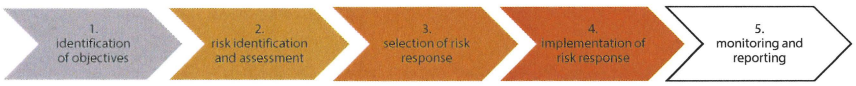
- *Judging whether certain risks can or must be accepted:* there are many reasons why certain risks have to be accepted. Firstly, taking risks is a necessary part of keeping an organisation dynamic and adapting it to a changing environment. It may also be necessary to accept a certain level of risk to achieve policy objectives (for example, research activities with a greater risk of failure may offer the highest benefits if they are successful). Secondly, certain risks are out of management's control and cannot be avoided without discontinuing the related activities (which have often been requested by the Legislative or Budgetary Authorities). Thirdly, reducing the risk to "zero" is usually not cost-effective.
- *Acceptable risk level ("risk tolerance"):* this is the total impact of risk an organisation is prepared to accept in the pursuit of its strategic objectives. The EPPO has to define its acceptable risk levels for quantifiable as well as for unquantifiable risk. Critical risks exceed

by definition the acceptable risk level and require action (unless the risk mitigation would be out of the management scope for action (e.g. external factors)).

- *Quantifiable risks:* for those activities where risk exposure can be quantified, management should reach a judgement on whether this level is acceptable. This assessment should be carried out at activity level. In all cases, a specific assessment of the financial impact linked to an action needs to be carried out. This assessment should take account of the possibility that further reduction of financial exposure may lead to excessive control costs - in other words: in pure financial terms, it is worth carrying out additional controls as long as each additional Euro spent on controls leads to a reduction of the error of more than one Euro.
- *Unquantifiable risks:* it may not be possible to quantify financial exposure for some risks due to their nature (for example those where the potential impact is largely reputational). Exposure for these risks needs therefore to be defined by reference to an appropriate measure such as reputational impact or regulatory compliance. For certain unquantifiable risk areas, a "zero tolerance" approach might be adopted e.g. security of staff.

2.4. Implementation of the risk response (action plans)

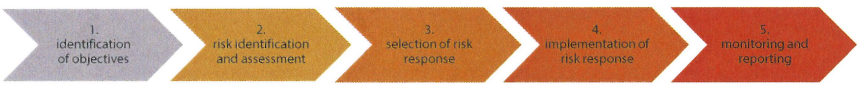
What concrete actions are needed to address the risks?



- *Establishing and implementing action plans:* in order 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-likelihood of the risk. As a minimum, the action plans should include a description of the risks and the actions to be taken, the owners of these actions (who will be responsible for implementing the defined measure(s)) and target dates/milestones.

2.5. Monitoring and reporting

Do the action plans remain relevant and effective?



- *Monitoring the implementation of action plans to ensure they continue to be effective and relevant:* Identified risks may evolve and new risks may emerge that could make the actions less effective or inadequate. Regular monitoring (e.g. quarterly) is therefore needed on the part of management, overseen by the Internal Control Officer for the most important risks.
- *Reporting on implementation of action plans is done in the Annual Activity Report.* Since the Annual Activity Report is public and should not include sensitive information, it does not include specific information about individual risks but only more general information

about key activities including how the overall risk levels have been managed. Moreover, for the risks that have materialised during the reporting year, more detailed disclosure is required including an assessment on whether or not a reservation to the Authorising Officer's Declaration of Assurance is required.

3. Risk Management in practice

3.1 Planning and organisation

3.1.1. Skills and awareness

- *Knowledge is a Critical Success Factor:* managers and staff organising or participating in the Risk Management exercise must have sufficient knowledge of its purpose and main concepts and of the bases for assessing impact and likelihood. They should also be conscious of the relevance of risk assessment to the work programme and achievement of objectives to avoid the incorrect perception that Risk Management is a purely administrative burden without much value.
- *Risk Management training (EULearn):* DG BUDG offers two Risk Management courses: (1) "Introduction to Risk Management and Internal Control" and (2) "Risk Management". The Introduction to Risk Management and Internal Control course is intended to provide a general understanding of the Commission's approach to Risk Management and Internal Control, introducing the concept of risk and the Risk Management process in the Commission. The other module is a hands-on course focused on the Risk Management process in practice and the Risk Management tools. Exchange of experiences and good practices are key elements in all the courses.
- *Risk Management seminars:* organising Risk Management seminars can be an effective way of raising management's and staff's awareness. The Internal Control Officer can also animate general or targeted risk assessment exercises.
- A range of useful information regarding Risk Management is available on BudgWeb.

3.1.2. Coordination

- *Flexibility:* the Risk Management exercise can be coordinated in different ways. The annual exercise should be interlinked with the Single Programming Document process, while at the same time ensuring its continuous nature to facilitate reaction to a changing risk environment. In general, the Internal Control Officer is the centre of competence providing technical advice. She/he facilitates the Risk Management process and contributes to the reporting. She/he is also a contact point for matters concerning Internal Control and Risk Management.
- *Documenting Roles and Responsibilities:* to ensure clarity and promote understanding within the EPPO, it is recommended to document the main roles and responsibilities related to the organisation and coordination of the Risk Management exercise.

3.1.3. Communication to participants

- *Involve management:* to be effective, the Risk Management exercise requires strong management involvement. Workshops, seminars and similar events can be organised to raise management's awareness of the Risk Management concept. Ideally, the Risk Management exercise should be announced and sponsored by the Administrative Director.
- *Presentations:* it is recommended to organise presentations or workshops at Unit level in which the purpose, basic concepts and practical arrangements are explained to the participants. Presentations or management meetings are generally more effective than using e-mails/websites alone.

3.1.4. Scope and approach

- *Management steer:* top management should steer the Risk Management exercise. This is primarily done by defining the scope, i.e. deciding what the annual Risk Management exercise should cover and deciding if there is a need to perform additional risk reviews of processes/projects/systems during the year.
- *Focus on higher-risk activities:* in general, the exercise should focus on activities or areas representing the highest risks, for example those that are new, have undergone significant change or have not been reviewed for a long period or for any other reason are considered to lead to a high residual risk level.
- *High-level review:* a high-level review may be used to identify activities or areas where a more detailed review is necessary (targeted review).
- *Targeted review:* top management may decide at the outset to focus the risk assessment on certain activities or areas. Under such an approach, "low-risk areas" - typically stable and well known activities - are excluded from the scope. It is also possible to target the review by building it around "risk themes" defined by top management.
- *Bottom-up perspective:* however, top management does not always have sufficient information about the Units' risks and may thus decide not to limit the coverage of the Risk Management exercise. In that case, an extensive review covering all main activities and objectives down to Unit level may be an option (an extensive "bottom-up" approach). Such a bottom-up exercise is likely to increase the number of risks identified and its advantage is that it is generally more comprehensive than a top-down approach.
- *A balanced approach:* the approach and degree of top management steer may vary and may change over time.

3.1.5. Stating outputs and activities related to objectives

Potential threats that could impact upon the achievement of the objectives of the EPPO are identified and corresponding mitigating actions are defined as part of a critical risk assessment exercise.

- *Activities or objectives/ outputs:* According to the Risk Management principles, "objectives" / outputs (what should be achieved?) are generally preferred to "activities" (description of foreseen actions) as a basis for risk identification. However, in practice, as activities are defined as the means to achieve objectives / outputs, and as indicators aim at measuring

progress towards achieving the objectives, any of the elements (objectives/ activities/ outputs/ indicators) can be used as considered appropriate by management.

- *Define objectives and related to them actions and outputs clearly:* in any case, the objectives/ activities/ outputs/ indicators used for risk identification must be clearly defined. If they are unclear or vague, the risks identified will also be likely to be unclear and vague. Objectives/ activities/ outputs/ 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:* the identification of risks is usually based on desk-reviews, followed by questionnaires, interviews or brainstorming sessions. The table below briefly describes these methods and points out their main advantages and disadvantages.
- In a multi-annual planning environment, risks linked to ongoing actions should be carried forward automatically from one year to another but re-assessed for the upcoming programming exercise.

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.	+ Already available information - Often deal with existing and already known problems - not so much focus on possible future risks or those which are not well-known
Questionnaires: All persons participating in the risk identification exercise are invited to complete a Risk Management questionnaire (pre-filled or blank).	+ A high number of persons can provide their input - Possible misinterpretations of input provided. - Using pre-filled questionnaires does not push for creative thinking (too much focus on risks proposed in the questionnaire). - Risk of low response rate - Can be perceived as "bureaucracy"

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.	+ Less risk for misinterpretations of input. + Opportunity for raising Risk Management awareness. - Risk that interviewer involuntarily bias the information obtained. - Relatively time consuming.
Brainstorming/Workshops: The Internal Control Officer organises brainstorming sessions with relevant managers and staff.	+ Exchange of ideas and experiences. + Opportunity for raising Risk Management awareness - Brainstorming sessions may be dominated by a few "strong voices" and certain persons may not want to give their frank opinion publicly.

- *"Fresh eyes":* in order to avoid carrying out successive Risk Management exercises in a routine manner (possibly resulting in the detection of few "new" risks…), it may be useful to change risk identification methodology from one year to another and to involve different staff if this is feasible.
- *Use of the common risk typology*: there are many types of risks, both internal and external. Whereas some risks may lead to issues regarding compliance with applicable rules and regulations, others may affect the operational effectiveness or safeguarding of assets and information. The mandatory Commission risk typology (see **Annex I**) is there to ensure that the most common risk aspects are covered and that the risk categories used are consistent across all the units. The common risk typology, used by both management and internal auditors, has three purposes. Firstly, it creates a common Risk Management language to facilitate communication. Secondly, it is a tool that can be used in the risk identification phase to help management make sure that all risks aspects and potential risk areas have been considered. And thirdly, the risk typology can be useful when analysing, consolidating and reporting risks.
- *Formulating the risks clearly:* in order to prepare for the subsequent assessment of the risks, it is essential that they are clearly defined and formulated, i.e. what is the main cause of the risks (what are the underlying problems?) and what are the potential consequences should the risks materialise (how would it impact the activities or objectives)?
- *Ensuring completeness of the exercise scope, including encompassing the risks of fraud:* when designing and running an overall risk assessment exercise, it is necessary to ensure that all types of potential risks are adequately considered. Managers naturally tend to focus on the operational risks, which they confront in day-to-day management, while not considering risks in the margins of their vision range. This problem can be addressed by ensuring that the sample of contributors is sufficiently representative of all professional functions as well as all domains, areas and processes managed by the organisation.

  In this context, it is worth recalling that some compliance risks may often be solely taken into account from an error perspective whereas they should also be considered for

potential fraud implications, thus deserving a more specific approach[3] within the overall and comprehensive risk exercise. In addition, it should be noted that the results of the Fraud Risk Assessment (FRA), undertaken as part of the update of the Anti-Fraud strategy, should be cross-referenced with the annual risk exercise to ensure completeness.

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

External partners' (institutional stakeholders - including Parliament and the Member States, contractors, beneficiaries, EU citizens etc.) views can and should be taken into account in the risk identification process where relevant.

Their opinion might be sought for example through the following measures:

a) surveys e.g. on the quality of service, payment deadlines, proposed new legislation;

b) review of recent complaints to the Commission/ Ombudsman;

c) European Court of Auditors' reports/ Discharge resolutions;

d) dialogue with the Member States' national administrations.

The list above is not exhaustive. It is to the responsibility of the Administrative Director to decide on the sources of information best adapted to the internal organisation and type of activity. Care should be taken before incorporating them into the risk assessment to ensure that external partners' views are relevant to the EPPO's objectives.

3.2.3. Risk assessment

- *Focus on the most significant risks:* the aim of the Risk Management exercise is to make sure that the most significant risks are adequately managed. It is not practically feasible to deal in detail with each and every risk identified and in fact the residual risk in many areas may already be at an acceptably low level. Fraud risks should in any case be analysed in detail and considered as potentially significant risks.
- *Assessments at different levels:* in order to single out the most significant risks, assessments should be organised at different levels. In addition to analysing and prioritising the risks communicated by the units, top management should identify additional risks, typically of strategic or high-level nature.
- *Preparing workshops:* in most cases, the risk assessment is performed via workshops/management meetings at different levels and prepared by the Internal Control Officer. The preparation usually consists of reviewing the risks identified, regrouping them in themes and, if there are too many risks, making a pre-selection of risks to be assessed in the workshop. For practical reasons, the number of risks dealt with in a workshop should be limited to 10-15.

[3] Fraud cases are characterised by patterns usually involving misrepresentation, falsified or forged documents thus clearly indicating the intentional nature of the acts which cannot be considered as simple 'irregularities'. However, controls aimed to ensure legality and regularity (compliance), usually also mitigate the risk of fraud.

- *Keep it simple*: the impact/likelihood approach is used when assessing risks. A scale from 1 to 5 must be used to assess both impact and likelihood of risks. However, this methodology should be used in a simple and pragmatic way. It should rather be regarded as a way of triggering a structured discussion about the risks than as a means of establishing precise "risk levels". Since most assessments are based on subjective judgements, quantified risk levels alone can give a false indication of precision whereas their value is to rank different risks. What is important is to understand the rationale behind the risk rating and, based on this information, determine if further investigations are needed.
- *Using voting tools*: using interactive voting tools is sometimes an effective way of assessing risks. It may lead to a more focussed discussion since the collective voting results and diverging opinions are clearly displayed.
- *When organising workshops, keep the following in mind*: the aim of a workshop is to bring together people, ideally from different levels and functions, with various experiences, in order to gather the group's collective knowledge on a certain topic - and the associated potential risks - and reach a common agreement on the subject. Workshops can either be of a "brainstorming" nature, when the objective is to identify risks/action plans, or structured around pre-selected risks when an assessment or a validation is needed. To be effective, workshops should not last more than 2-3 hours and should generally not involve more than 10-12 persons.
- *The workshop should integrate full risk assessment* i.e. not only focus on risk identification but also on identification of existing controls and assessment of their effectiveness, risk response and action plan.

Table 2: Tips for conducting a workshop

Prior to the workshop

√ Designate the Internal Control Officer to prepare and manage the workshop

√ Define clearly the scope and purpose of the workshop

√ It is crucial that the risks to discuss are well defined and formulated (not applicable in case of "brainstorming" exercise)

√ Ensure that the workshop is well-balanced in terms of skills, knowledge and experience

√ Establish a workshop agenda

√ Announce the workshop to the selected participants in due time

√ Ensure that all participants are informed about the scope and purpose

√ Ensure that the participants have sufficient knowledge about Risk Management principles

The workshop itself

√ Stick to the workshop agenda

√ Focus the discussion on the impact/likelihood of the risks

√ Use voting tools or other methods that can facilitate reaching a consensus

√ In case of non-consensus, top management - ultimately the Administrative Director - will take the final decision

After the workshop

√ Document results and conclusions

√ Keep participants informed and communicate the results and conclusions to them.

3.2.4. Critical risks

- *Mandatory reporting*: The critical risks must be reported in the Annual Activity Report and the Single Programming Document. It is always the residual risk level and not the inherent risk level that should be taken into account in defining criticality.
- Overall EPPO perspective: the identification of critical risks should be carried out from an overall-EPPO perspective. This is to ensure that the assessment is balanced and complete.
- *Formal validation of risks*: the Administrative Director validates the critical risks. In addition, he/she should validate other significant risks via management approval of risk registers or action plans.
- *Sensitive risks*: certain critical risks are of a sensitive nature, for example if they concern security-related issues or third parties. Care should be taken when formulating such risks and referring to them in the AAR so that no damage is caused to the EPPO or its partners.
- *Link critical risks/AAR:* a critical risk can become a reservation in the subsequent AAR if not adequately managed. Likewise, a Risk Management action plan will need to be developed for reservations in the AAR of year n-1. Reservations of year n-1 could also be taken into account when assessing the criticality of the risks in year n.

3.2.5. Cross-cutting risks

For critical risks which are *potentially* cross-cutting, peer reviews are organised with the units concerned to gather detailed information, estimate the risk level and assess at what organisational level the risk would be best managed, assign a chef de file and establish an action plan. Accordingly, the designated lead service is responsible for ensuring delivery of the actions decided upon.

3.2.6. Risk inter-dependencies

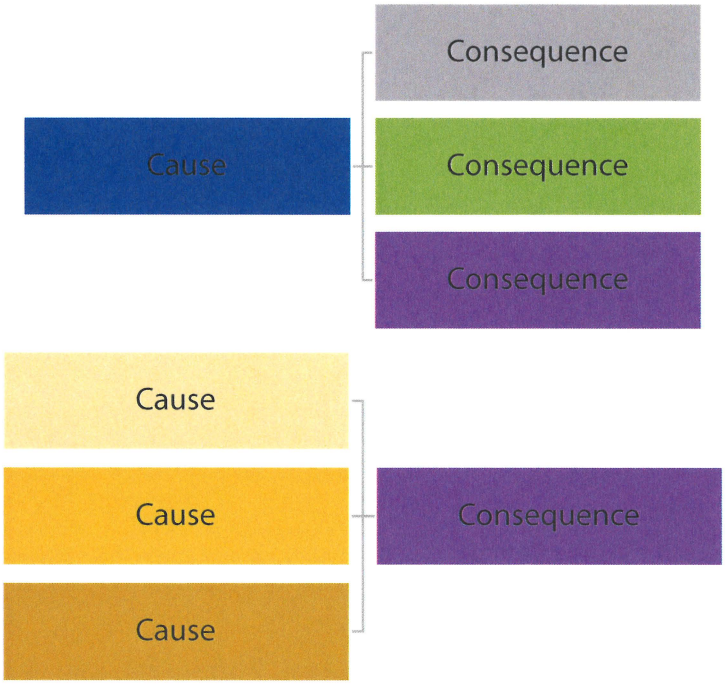
a) Risk identification

Cause → Consequence

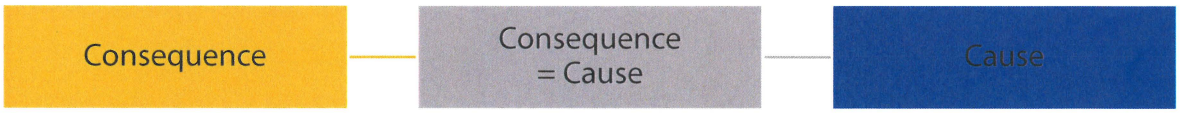
Note that when identifying a potential event which might be the cause of risk, care should be taken to define all the risks which might result from it. In other words: several risks might result from one cause. And the other way round: the risk may materialise only if several events which were defined as a cause happen at the same time.

Both situations are illustrated by the following diagram.

Risk inter-dependencies



Consequence (i.e. materialisation of risk) might at the same time be the cause for another risk.



b) Risk assessment

Attention should be paid in assessing the most important risks to identify any consequences on other activities of the EPPO:

Example:

If risk A is simultaneously the cause for risk B and the likelihood of occurrence of risk A is low → probably the likelihood of occurrence of risk B is also low.

c) Risk response

The defined risk response might have an effect on the materialisation of another risk e.g.

- acceptance of risk A might result in an increased likelihood of occurrence of risk B (for example a high workload in the unit may result in significant staff turnover in the future). Management accepted the risk ranking it as 'low likelihood'. However if the risk

materialises, the relationship with stakeholders - e.g. a contractor developing an IT system - may deteriorate, reducing the quality of the contractor's own output and reducing the EPPO's capacity to deliver on its objective of introducing the IT system on time).

- mitigation of risk A may result in a higher probability of risk B materialising (e.g. implementation of the new IT system to fight fraud could result in a higher workload for staff which may result in staff dissatisfaction and leaving of the EPPO).

Risk inter-dependencies may be identified at each stage of the risk management process and the examples given above are illustrative. Therefore care should be taken to ensure that inter-dependencies between risks are identified and are regularly followed-up.

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 fall mostly under category 1 ("Risks related to the external environment") of the Commission's Risk Typology (**Annex I**). In the case of most of these risks the only possible answer is usually "*Accept*", though some measures to mitigate the impact may be possible. As a result of the lack of direct control over this type of risk, they should be monitored on a more frequent than annual basis (preferably quarterly) in order to:
  - verify and confirm the risk categorisation (critical, important, low risk).
  - verify whether they are still outside management control and identify possible further measures to mitigate impact.

Examples of risks which may be outside management's control:

- sudden crisis, political instability, economic weakness, natural disaster, health crisis;
- failure of the engagement of Member States, authorities and stakeholders in the achievement of shared objectives;
- the risk of delays in implementation of one of the crucial IT systems due to underperformance of an external contractor.

3.3.2. Risk registers

Risk register = Overview of the most significant risks

Action plan = Detailed and concrete measures to be taken to implement the risk response

- *Overall EPPO risk register:* documenting the EPPO's most significant risks in a central risk register is mandatory. Typically, the risk register should include all the significant risks identified in the EPPO (including the "critical risks").

- *Unit risk registers:* in addition, it may also be useful to document each Unit's most significant risks in separate risk registers.
  - *Risk register format:* the risk register should contain as a minimum the following information:
    - risk description using the "cause - consequence" model. The risk level recorded should be assessed at its residual level (after controls existing in the organisation)
    - inherent risk level (optional – see explanation below)
    - risk type as per risk typology
    - classification of a risk that could (also) be the result of fraudulent behaviour
    - policy area/activity/objective affected by the risk
    - general objective affected by the risk (only if applicable)
    - proposed risk response
    - action plan (actions, owner, deadline).

Optionally the units might also include other information, such as: inherent risk level, controls in place, etc. While it is a rule that risks are assessed always at their residual level, it is recommended to regularly re-assess the most apparent inherent risks, in order to conclude whether related mitigating controls are still effective/should be enhanced/reduced. However, a regular risk assessment exercise should not take inherent risk level as a starting point for assessment, as this would significantly increase administrative burden with little added value.

- *Keep risk registers updated*: risk registers should reflect the implementation of action plans and the emergence of new risks. The updating should be carried out on a continuous basis (that is, as and when some aspects change) by the responsible managers and monitored by the Internal Control Officer.

3.3.3. Action plans

- *Action plans:* establishing clear and comprehensive action plans which clearly allocate responsibility for and timing of action is essential for effective Risk Management. They are needed to make sure that risks are addressed in line with management's instructions, and constitute the benchmark for monitoring progress. Adequate action plans are particularly important for actions spanning a long period (for example major projects).
- *Action plan format:* there are no mandatory requirements for action plans: the important thing is that they identify clearly what needs to be done, by whom and by when. It is recommended to include: risk description, action plan goals, target dates and milestones, action owners, specific actions to be taken, resources needed and monitoring/reporting arrangements.
- *Monitoring:* regular monitoring of the implementation of action plans is needed for two purposes: (1) to ensure the actions are progressing according to plan; (2) to ensure that the planned actions remain relevant. Identified risks may evolve and new risks may emerge in which case action plans must be modified accordingly.

- *The practical organisation*: in general, action plans are supervised by the responsible managers. Central monitoring of the risk register should be performed by the Internal Control Officer.
- *Coverage*: the monitoring of action plans should not be limited to the critical risks, but should also cover other significant risks in the EPPO (for example the top 10-15 risks). If the monitoring of such risks is insufficient, and they increase in importance in the future, management may be slow to react due to a lack of regular information.
- *Reporting*: the results and conclusions of the monitoring should be documented and reported to the relevant management level. The Administrative Director should be kept informed of the evolution of critical risks.

3.3.4. Contingency plans for accepted critical risks

Occasionally Management can decide to accept a risk which is of critical nature (even after mitigating measures have been defined). This can happen in two cases:

a) the risk is out of Management's control (i.e. external risk) – e.g. the risk of economic crisis, the risk of pandemic, the risk of corruption in third countries.
b) it is a deliberate Management's decision to take the risk.

In both cases the EPPO must define a follow-up (contingency) plan offsetting out the actions to be undertaken if the risk materialises.

The accepted critical risks at the level of the EPPO/ the unit should be covered by a dedicated contingency plan, which defines as a minimum:

- the person responsible for decision-making
- actions to be taken (and their owners) to minimise the impact on the EPPO should the risk materialise
- other units involved in a contingency plan should the risk materialise

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

3.4. Specific risk reviews

- *A continuous process:* in addition to identifying risks as part of the programming process, it is recommended to carry out more detailed risk reviews of specific key processes/projects/systems during the year at times which are judged appropriate in the planning and execution cycles of the activity concerned.
- *Same basic principles:* when conducting specific risk reviews of processes/projects/systems, the fundamental Risk Management principles apply, namely:

1) Defining activities and objectives (e.g. what is the process/project/system supposed to achieve?);

2) Identifying and assessing risks using the impact/likelihood method;

3) Deciding how to deal with the identified risks taking into account "acceptable" risk levels;

4) Establishing and implementing actions plans; and

5) Following-up the implementation of action plans.

- *Coordination:* typically, project managers or concerned line managers are responsible for coordinating and carrying out specific risk reviews. They are assisted by relevant staff (and the Internal Control Officer where appropriate) and if necessary by external specialists.
- *Scope and timing*: compared to the Risk Management exercise performed annually, as part of the programming process, the scope of a specific risk review is generally more detailed. Depending on the complexity and size of the process/project/system, the length of the review may vary from a couple of days to several weeks.
- *Coherence:* In all cases, the Internal Control Officer should be informed of a specific risk review to keep the coherence of the EPPO risk management.
- *Flow-charting:* in order to prepare for the risk review, it is recommended to graphically illustrate the concerned process/project/system, for example by flow-charting. This facilitates the definition of the scope and serves as a basis for the risk identification. The scope of the risk review can include all or only certain phases of the process.

ANNEX I: RISK TYPOLOGY

The EPPO's risk typology is mandatory and all risks must be 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		
Main risk groups		Areas to consider when identifying potential issues and risks
External	**1. Risks related to the external environment (outside the 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**	- Strategy, planning and policy, including internal political decisions; - 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, competences, 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, buidlings 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 timelines of information

ANNEX II: RISK REGISTER

Risk title and description (including cause and potential consequence)	Risk type	Policy area & activity/specific objective affected	General objective affected	Inherent risk level	Residual risk level	Risk response	Action plan summary		
							Brief description	Owner	Deadline

Glossary

- **Critical risk**: a risk should be considered critical if it can:
  - jeopardise the realisation of major policy objectives;
  - cause serious damage to the EPPO's staff, partners or customers (Member States, companies, citizens, etc.);
  - result in critical intervention at political level (Parliament, Council, Commission) regarding the EPPO's performance;
  - result in significant infringement of laws and regulations;
  - result in material financial loss;
  - put the safety of the EPPO's staff at risk;
  - in any way seriously impact the EPPO's image and reputation;
  - the risk should also be considered as "critical" if the combination of its impact and likelihood falls in the upper end of the scale of the impact/likelihood model.

- **Cross-cutting risks** are critical risks which affect several units and can be evaluated or addressed more effectively at organization level.

- **Impact** represents the effect on the objectives/activities in case the event or issue giving rise to the risk occurs.

- **Inherent risk:** the risk related to the very nature of the organisation's activities.

- **Likelihood** represents the probability that, or frequency with which, an event is expected to occur over a given time horizon.

- **Most significant risks** are significant risks, which in view of Management can become critical in the future.

- **Objective** represents what the EPPO (or a unit within the EPPO) wants to achieve (e.g. political, strategic, and operational).

- **Residual risk** is the risk remaining after the controls put in place to mitigate the inherent risk.

- **Risk** represents any event or issue that could occur and impact the achievement of the EPPO's political, strategic and operational objectives. Lost opportunities are also considered as risks.

- **Risk map:** a graphical presentation of likelihood and impact of one or more risks. Risk maps may plot quantitative and qualitative estimates of risk likelihood and impact. Often risk maps are referred as "heat maps" since they present risk levels by colour.

- **Acceptable risk level:** the total impact of risk an organisation is prepared to accept in the pursuit of its strategic objectives.

- **Risk assessment** is the overall process of risk identification, analysis and evaluation; sometimes it is used in a more limited context to refer solely to risk definition of its impact and likelihood of occurrence.

- **Risk level** is the result of the combination of the likelihood that a risk occurs with its impact should it occur.

- **Risk Management** is a continuous, proactive and systematic process for identifying, assessing and managing risks in line with the accepted risk levels, carried out at every level of the EPPO to provide reasonable assurance as regards the achievement of the objectives.

- **Significant risk** represents a risk that could have a significant/material impact on the EPPO's objectives/activities.

Contacts and references

For further information on Risk Management, the following sources can be consulted:

- The Communication on Risk Management SEC(2005)1327
- BUDGWEB: Reference documents and detailed guidance for the practical implementation
- BUDG/CFS/D3: Contact via mail to BUDG MAILBOX D03 if you have any specific questions regarding Risk Management and Internal Control
- COSO-ERM: The principles of the Commission's Risk Management methodology are based on the internationally recognised COSO-ERM framework