



## EUROPEAN COURT OF AUDITORS

AUDIT METHODOLOGY AND SUPPORT UNIT

# RISK ASSESSMENT IN PERFORMANCE AUDITS

## TABLE OF CONTENTS

### Section 1: What is risk assessment & when to perform it

1.1 The purpose of risk assessment

1.2 Defining risk and risk assessment

### Section 2: How to do it

The auditor's approach to risk assessment

Step ① - Present the audited area in a diagram & list the expected key controls

Step ② - Identify the risks

Step ③ - Analyse the risks to assess the risk level

Step ④ - Focus on the key risks to define the audit questions and scope

### Annexes

I: Risk Assessment Process

II: Sources of information

III: Illustrative list of risks factors

IV: Examples of risks

## FOREWORD

The Performance Audit Manual of the European Court of Auditors states that "the preliminary study<sup>1</sup> should analyse the relative significance of the risks to sound financial management, which will help to provide focus for both the potential audit questions and audit scope". The purpose of this guideline is to provide the auditor with:

**Guidance** for carrying out risk assessment in order to identify and analyse the risks to sound financial management, and allow a more structured approach to developing relevant audit questions.

**A template** to document the result of the risk assessment.

**Section 1** gives a brief introduction to the method, its key concepts and tools, and discusses its main features and when to use it.

**Section 2** is a detailed guide for the auditor on how to perform risk assessment in the planning of a performance audit.

*A case study, illustrating how a risk assessment is carried out in practice, is annexed to this guideline. The case is adapted from the audit on Translation Expenditure of the Institutions<sup>2</sup>.*

### List of related documents

[Risk\\_my\\_audit.xls](#) (template)

### Whom to contact

If you feel that the information provided in this document could be improved, please do not hesitate to communicate your suggestions:  
ECA-AMS.CONTACT@eca.europa.eu.

<sup>1</sup> The purpose of the preliminary study is to enable the responsible Member to assess whether the audit is realistic, realisable and like to be useful. The emphasis is on testing the availability of information and the feasibility of methods.

<sup>2</sup> Special Report no 09/2006 on the translation expenditure incurred by the Parliament, the Commission and the Council.

## SECTION 1: WHAT IS RISK ASSESSMENT & WHEN TO PERFORM IT

### 1.1 THE PURPOSE OF RISK ASSESSMENT

**Perform risk assessment during preliminary study**  
to focus the audit on high-risk areas.

The Performance Audit Manual requires the auditor to perform risk assessment **during the preliminary study** in order to:

- reveal areas of potential weakness in an organisation,
- identify risks and analyse those which are the most significant and critical to the achievement of good performance,
- examine how risks are managed by the organisation,
- focus the audit on areas of high risk and develop related potential audit questions.

Following the risk assessment, the auditors will complete the **Potential Audit Question and Scope (PAQS) table**, a tool which will help in choosing the high-level question(s) for the audit and in defining the audit scope.

### 1.2 DEFINING RISK AND RISK ASSESSMENT

#### What is risk?

**Risk** can be defined in various ways, depending on the context. Generally, risk is considered as the possibility of loss or injury, a threat of something going wrong with the activities or organisation of the entity or persons concerned. In the EU context, the auditor deals mostly with organisations and programmes which have policy objectives. Therefore, an objectives-based definition of risk is the most suitable.

Risk is thus defined as an incident or the occurrence of a particular set of circumstances that, if they occur, could adversely affect the organisation, such as exposure to financial loss, loss of reputation or failure to deliver a policy or programme economically, efficiently or effectively. Risks may vary in nature and concern any level of the organisation.

**Risks to sound financial management**, i.e. risks to achieving economy, efficiency and effectiveness, can be inherent in nature (inherent risk) and/or arise from weaknesses in internal control (control risk). The inherent risk is the risk level before existing controls and/or risk response. Residual risk is the risk level still remaining after taking existing actions and controls into account.

#### What is risk assessment?

A general definition of **risk assessment** is "the identification and analysis of relevant risks to the achievement of objectives, forming a basis for determining how the risks should be managed".<sup>3</sup>

In the context of a performance audit, risk assessment can be defined as the identification and analysis of the key risks to the achievement of objectives concerning economy, efficiency and effectiveness, thus forming a basis for developing potential audit questions and determining the potential audit scope.

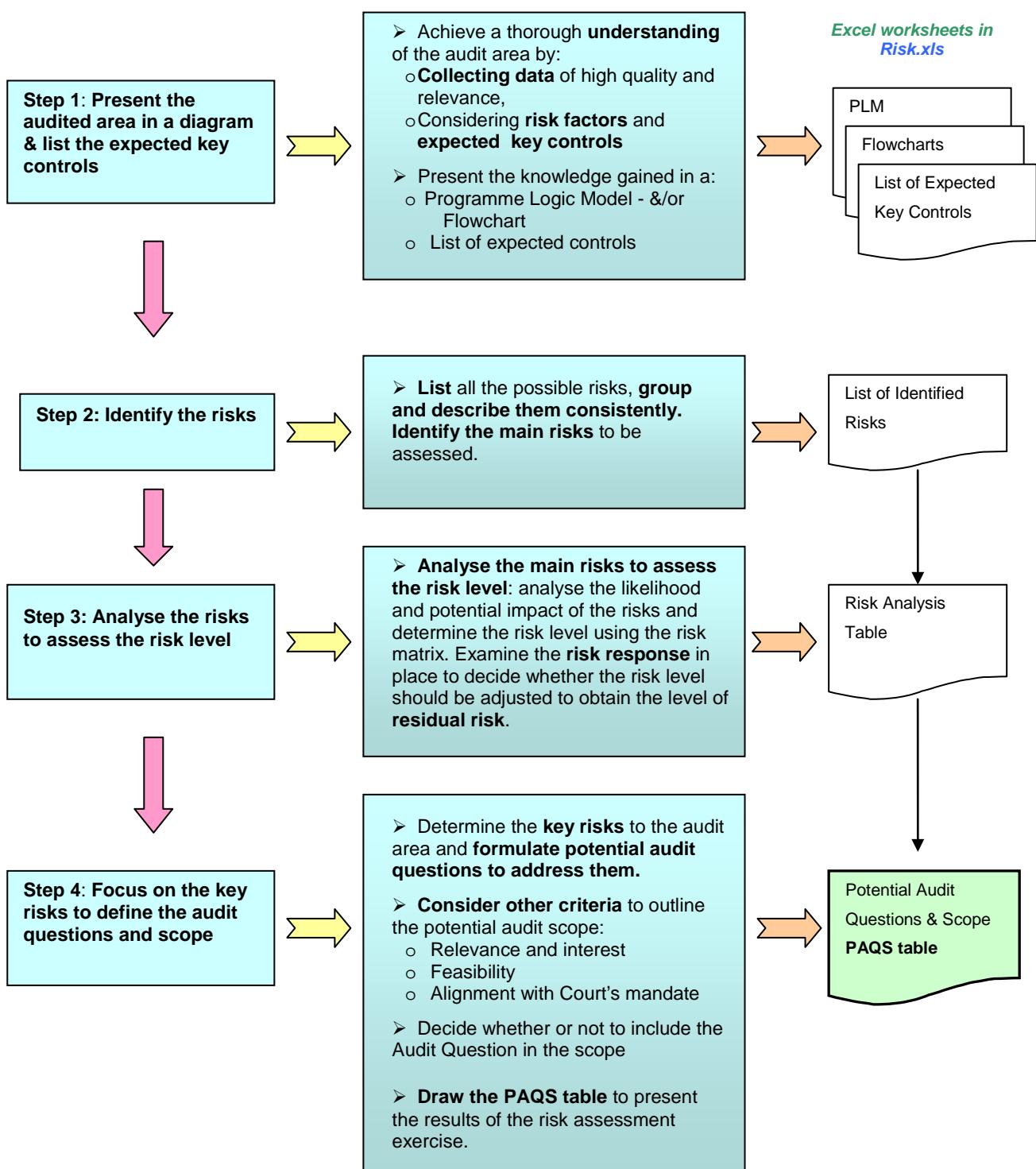
<sup>3</sup> Enterprise Risk Management - Integrated Framework, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004.

## SECTION 2: HOW TO DO IT

### In four progressive steps.

The risk assessment process consists of four progressive steps, each step acting as a filter and leading to the next. This allows the auditor to start with the acquired knowledge of the audit area and to eventually focus on the key critical risks that lead to relevant potential audit questions and potential audit scope. (see **Annex I: The risk assessment process: input, tools and output**)

#### Overview of the risk assessment process

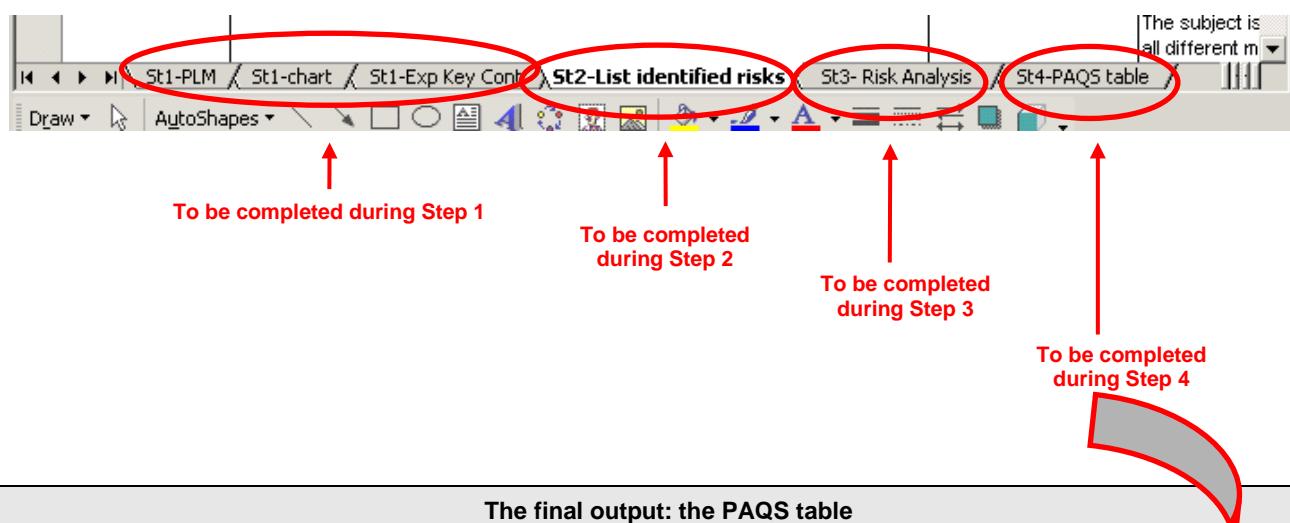


## The auditor's approach to RISK ASSESSMENT

Risk assessment should be the **link** between the knowledge acquired of the audit area and the audit questions and scope. Identifying and assessing risk is not an exact science and will mostly depend on the sound judgement of the auditor. This judgement should be based on knowledge, analysis and experience. The auditor has to be **systematic, comprehensive and rigorous**. No important risks should be overlooked.

## The worksheets in Risk\_my audit.xls

The decision-making process throughout the risk assessment should be recorded in Risk\_my audit.xls to enable reviewers and management to fully understand the process. The Risk\_my audit.xls template has been built to reflect, step by step, the auditor's analysis and judgement throughout the risk assessment exercise. Each step of the process has a dedicated sheet(s), leading to the final output, the **Potential Audit Question and Scope** or PAQS table.



The purpose of the **PAQS table** is to give an overview of:

- the final assessment of the risks,
- the audit questions which can address them,
- the relevance, interest and feasibility of the audit questions, and thus,
- one, or more, potential audit scope(s).

The **PAQS table** is a **tool** to define the audit scope. It will be composed as follows:

Results of the auditor's assessment		Information needed to focus the audit.			Audit scope	
Area/ Objective/ Activity/ Process /	Key Risk	Residual Risk level H-M-L	Audit Question	Relevance & Interest H-M-L	Feasibility Normal Difficult Not Feasible	To be included in Scope Yes-No
xxxxxx						
xxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	H	xxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	Y
xxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	H	xxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	Y

## STEP ① - PRESENT THE AUDITED AREA IN A DIAGRAM & LIST THE EXPECTED KEY CONTROLS

The objectives of this step are to acquire and present a comprehensive and coherent knowledge of the audit field and to identify the controls that are expected to be in place. To this end, it is suggested to present the area in a **Programme Logic Model** (PLM)-chart and/or in flowcharts and to prepare a list of expected controls.

**Acquire a sound and up-to-date knowledge,**

The basis of any risk assessment process is to have a sound, up-to-date knowledge of the audit area, irrespective of the size and nature of the subject. The auditor should acquire and demonstrate **a thorough understanding of the policy/programme/entity's objectives** and related success indicators, of the key actors, processes and key controls.

**collect high quality data,**

Relevant **quality data** provides a valuable base from which to identify risks to sound financial management. Sources of information include the auditee itself, external stakeholders (beneficiaries, users, non-users, etc.), the Court's own documents and reports from the European Commission or other European Institutions, Supreme Audit Institutions or public bodies.

**and consider risk factors.**

Examples of documents and organisations that can provide the auditor with additional information on the audit area are given in **Annex II**.

Special attention should be given to **risk factors**, i.e. certain conditions that may increase the risk level, which requires a more in-depth knowledge of the area in order to achieve a more extensive assessment of potential risks.

An illustrative list of risk factors is provided in **Annex III** (auditors could also use the risk factors identified in the Programming exercise for establishing the Portfolio of Potential Audit Questions). The auditor can add to this list the risk factors which are specific to the audit area.

**Present the knowledge acquired in a diagram,**

The knowledge acquired by the auditor needs to be presented in a diagram, which gives a comprehensive overview of the audit area. The auditor is encouraged to build a PLM to set out the logic of the public intervention.

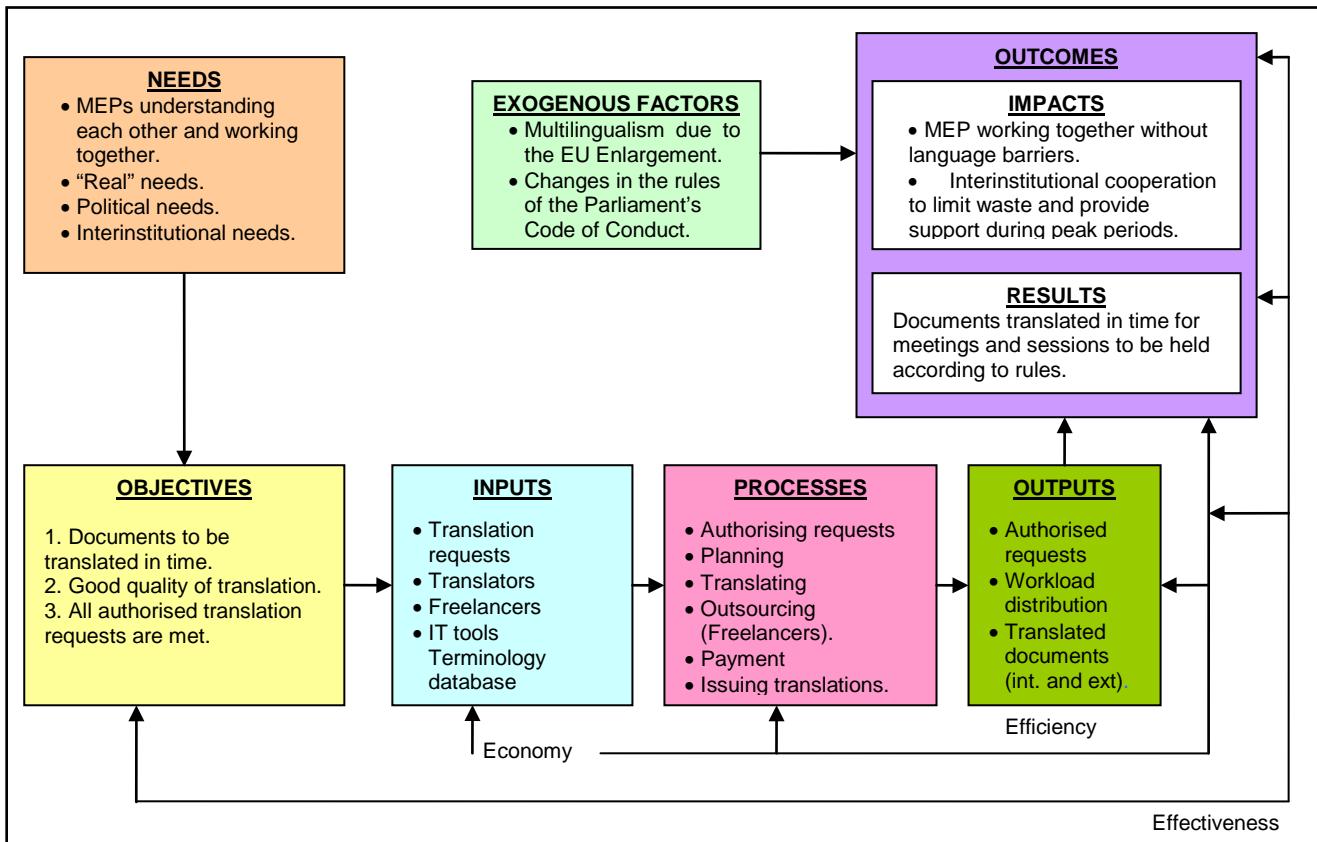
**and/or in a flowchart.**

The PLM, proposed in the Court's Performance Audit Manual<sup>4</sup>, helps to identify and set out the relationship between the socio-economic needs to be addressed by the intervention and its objectives, inputs, processes, outputs and outcomes, which include results and impacts.

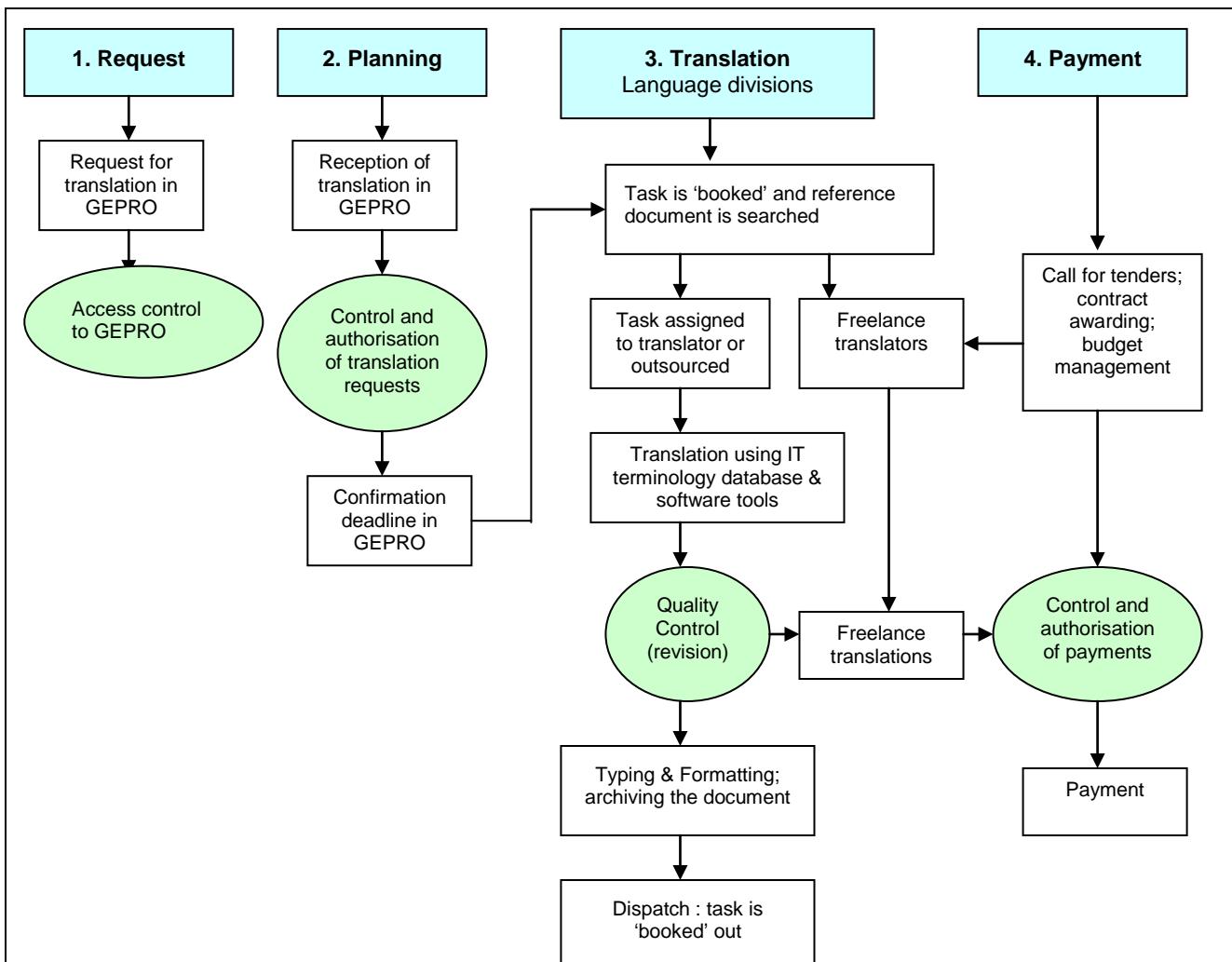
The auditor may need to present one or more elements of the PLM at a more detailed level. (S)he can use a flowchart to do so. Flowcharts are maps or graphical representations of a process. Flowcharts are particularly useful for displaying how a process currently functions or could ideally function.

<sup>4</sup> Performance Audit Manual, Chapter 2, par. 2.3.1 The use of logic models in performance audits.

 Example of the Programme Logic Model adapted from the audit on the "Translation Expenditure of the Institutions"



 Example of a flowchart adapted from the audit on the "Translation Expenditure of the Institutions"



## List the expected key controls.

Once the processes have been displayed and understood, it is necessary to identify the key controls that an auditor expects to find. The controls can be briefly described in a **List of Expected Key Controls** (see below). Many control risks are derived from the lack or the malfunctioning of such controls. This list can also be used when building the Evidence Collection Plan.

 Example of a List of Expected Key Controls adapted from the audit on the "Translation Expenditure of the Institutions"

Area Objective Activity Process	List of Expected Key Controls
1. Requests	Proper authorization procedures. Rules adopted by the Parliament defining e.g. who can and who cannot require a translation, the number of pages accepted per type of request, deadlines. Exceptions to the rules clearly stated. Controls at the Planning stage to accept or reject requests. Controls at the level of each language unit to accept or reject a request. Monitoring controls and Management Information System: for example rejected requests by type and by DG, ratio of rejected requests over total number of requests, number of exceptions and their justification, requests submitted within the tabling deadlines and those submitted after the deadlines.
2. Planning	Controls that resources are proportionally spread between units and institutions. Controls that the text has not already been translated in the past. Controls that there is as little as possible idle time per translator. Translators are working on priorities and on the right tasks.
3. Translation	Heads of divisions should ensure that important translations are issued in due time. Quality control/ revision.
4. Payment	Controls ensuring that tendering procedures are compliant with Financial Regulation. Calls for tenders ensuring that best value-for-money offers are selected. Payment to freelancers: correct amounts, correct period, correct bank accounts. Budgetary needs properly forecast and followed up.

## STEP ② - IDENTIFY THE RISKS

### Develop initial ideas to list all possible risks.

The auditor should now identify the key risks. (S)he should first list all possible risks and then group, describe and select those which should be included in the Risk Analysis table in order to be analysed.

Ideas of risks can be developed by studying the **PLM**, the **Flowchart** and the **List of Expected Key Controls** built in Step 1 and answering the following questions:

1. What can go wrong? What can be the risk?
2. What assets are at risk - property, resources, information, reputation, legality?; from what sources – internal or external?; at which level: internal, external, legal, strategic, operational, organisational or administrative?
3. With whom does the risk lie?
4. What factors are / can be constraining performance (economy, efficiency, effectiveness)?
5. What could be the cause (including weaknesses in controls)?
6. What could be the consequences or the impact?
7. How could this risk be managed?

Initial ideas may also be developed during a **brainstorming session**. The session could be conducted by an independent colleague, acting as a facilitator, with a **limited number of participants**. It is often helpful to conduct the session with financial audit colleagues (preferably with auditors which have covered the area) or other experts.

### **Group ideas by categories.**

A first “raw” list of all possible risks must be closely examined, sorted and fine-tuned. Several distinctions can be made: i) between the inherent risks and the control risks; ii) between the high-level risks and the more operational or detailed risks; iii) between the significant risks and the other risks.

Risks can be grouped by affinity i.e. by category, by subject, by theme. Risks can also be sorted by different categories: objective, type, impacted area, root-cause, process, activity, etc. or any other criteria selected by the auditor and which is **relevant for the audit**.

#### Examples of risks by categories:

Category	Risk
<b>ECONOMY</b>	<ul style="list-style-type: none"> <li>• Waste</li> <li>• Overpaying</li> <li>• Gold-plating</li> </ul>
<b>EFFICIENCY</b>	<ul style="list-style-type: none"> <li>• Leakages</li> <li>• Non optimal input/output ratios</li> <li>• Slow implementation of the intervention</li> <li>• Failure to identify and control externalities</li> </ul>
<b>EFFECTIVENESS</b>	<ul style="list-style-type: none"> <li>• Faulty policy design: inadequate assessment of needs, unclear or incoherent objectives...</li> <li>• Management failures: objectives not being met, management not prioritising the achievement of objectives.</li> </ul>

A detailed explanation of the table above can be found in the Performance Audit Manual. Other examples of risks and risk categories are given in **Annex IV**.

### **Describe the risks consistently.**

Relevant selected risks should then be described in a consistent manner in order to be included in the “List of identified risks”. The description of a risk should ideally follow this equation:

$$\text{Risk formulation} = \text{cause} + \text{problem} + \text{impact}$$

Therefore, it should include the following information:

- what are the main **reasons** for the problem?
- what is the **problem**?
- what are the most important potential **consequences**?

#### Example of risk description adapted from the audit on the "Translation Expenditure of the Institutions"

Objective	
“Translating the “compte-rendu in extenso” <sup>5</sup> (CRE) in the “most recent” official languages in time to be published in the Official Journal”	
Risk Description	Assessment of risk description
“Failure to translate in time” ( <b>problem</b> ). “Lack of translators” ( <b>problem</b> ).	<b>Example of a bad risk formulation</b> because it does not include any indication of the cause or the impact of the problem
“Lack of translators for the “most recent” official languages ( <b>problem</b> ) can lead to delays in publishing the CRE in the OJ ( <b>impact</b> )”.	<b>Acceptable</b> because it gives an indication of the potential consequence. However, even when the information is not available, the auditor should try to give possible reasons for the problem.
“Due to insufficient recruitment ( <b>cause</b> ) translators for the “most recent” official languages are not available ( <b>problem</b> ), which leads to a risk of significant delay in the publication of the CRE in the OJ ( <b>impact</b> )”.	<b>Good</b> because both the cause and the consequence of the problem are clearly stated.

5 The minutes of the European Parliaments' session debates.

**Create the List of Identified Risks.**

The auditor should now be aware of all the risks relating to the audit area. The risks identified should be closely examined in order to decide on the ones that are key (significant and relevant). These risks must be included in the Risk Analysis table, where their likelihood and impact are assessed. The decision of not giving the risk further consideration has to be explained in the "Comments" column of the template.

 *Example of a List of Identified Risks adapted from the audit on the "Translation Expenditure of the Institutions".*

For the risks which the auditor decides to further analyse (answer Yes in 3<sup>rd</sup> column), these 2 columns are manually copied and pasted in the Key Risk Analysis table on the next sheet of the [Risk\\_my audit.xls](#) template.

Area/ Objective/ Activity/ Process	Description of Risk cause + problem + impact	Key Risk (to be included in Risk Analysis table for assessment) Y / N	Comments
HR	<b>General human resource and infrastructure management</b>	NO	The subject is too vast for an audit to encompass all different management aspects that can influence the cost and the efficiency of the activity. These aspects will be addressed indirectly.
HR	<b>Risk to the legality and regularity of the payments to the staff</b> and overhead costs for buildings and technical equipment in cases where the procedures are not followed.	NO	Covered by the annual financial and compliance audits.
<b>1. Requests</b>			
1.1	<b>Risk of linguistic over-consumption</b> in case that the authorization procedures don't avoid applicants resorting to translation more often than absolutely necessary, e.g. translation of less important texts, translation when the individuals involved have a sufficient knowledge of the source language, which increases the costs.	YES	
<b>2. Planning</b>			
2.1	<b>Risk of inadequate distribution</b> of resources between institutions and units, due to the absence of interinstitutional cooperation, resulting in contracting freelancers when the same or another institution has available in-house capacity.	YES	
2.2	<b>Risk of low productivity</b> because of uneven distribution of workload, inadequate management tools - translations are not finished in time, delaying meetings and court cases.	YES	
<b>3. Translation</b>			
3.1	<b>Risk of too much emphasis on quality</b> , due to the lack of clear instructions by management, which would result in less productivity of translated document.	YES	
<b>4. Payment</b>			
4.1	<b>Risk of irregular procedures</b> in the selection of freelancers and the assignment of jobs due to non-compliance with the rules of the financial regulation. Each Institution recruited separately without any call for tender as annual amounts paid to individual freelancers were beneath the threshold. Irregular procedures constitute an infringement to the rules for which the Institution can be sued.	YES	
4.2	<b>Risk of insufficient performance</b> - not all the freelance translations are subject to quality control and/or revision, which would cause translations of insufficient quality not to be sent back and corrected, and the contractual penalties in such cases not to be applied.	NO	Very improbable, based on the interviews held with the Heads of units.
4.3	<b>Risk of over - or under- payment</b> i.e. that the correct price per page is not applied and that the deadlines for payments are not respected, due to insufficient controls, resulting in waste of money.	YES	

## STEP ③ - ANALYSE THE RISKS TO ASSESS THE RISK LEVEL

### Analyse the key risks using the Risk Analysis table.

The auditor should only assess those risks identified as key in the previous step. To do so, (s)he will use the **Risk Analysis table**.

Risks should be prioritised according to their level (high, medium or low). The level of risk is obtained by assessing separately the likelihood of the event occurring and the impact of that event.<sup>6</sup> Then, the residual level should be determined by considering the management response to the risk.

The **accuracy of the risk analysis** will depend on the quality of the information available. Evidence should be used when it is available. Nevertheless, the auditor has also to rely on **common sense and sound professional judgement**, based on the knowledge acquired and on experience.

#### Tips!

- ⇒ The auditor should not aim for unrealistic levels of accuracy.
- ⇒ The time spent on quantifying risks should relate to their likely materiality.

#### What is the likelihood of it going wrong?

The auditor must decide on the **likelihood** of the risks materialising, which is the fundamental difficulty in risk assessment since statistical information is not available and rare failures are hard to estimate. When estimating the likelihood of an event, the auditor will inevitably work on assumptions. These assumptions should be reasonable and should be documented.

#### What is the impact?

The auditor then has to investigate how vulnerable the organisation is to the threats posed, and determine what is the **likely impact**, or consequences of the risks, on the organisation and/or the achievement of relevant objectives, should the risk materialise. The analysis of the consequences of risk should not be restricted to the direct effects only but should extend as far as possible.

#### Risk quantification: high – medium – low

The auditor should determine a level – **high, medium or low** – of occurrence (likelihood) and seriousness (impact) for each risk using the risk matrix below. The overall evaluation is the result of the combination of both elements.

$$\text{Risk} = \text{likelihood of occurrence} \times \text{impact of the event}$$

#### The Risk Matrix

		Impact		
		Low	Medium	High
Likelihood	Low			
	Medium			
	High			
Overall risk evaluation:		<b>Low</b> Risk can be ignored	<b>Medium</b> Judgement based on characteristic of defined risk	<b>High</b> Risk must be followed up by audit

<sup>6</sup> Enterprise Risk Management - Integrated Framework, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004.

**For medium and high risks,  
consider management response  
in place:**

**Is (can) the risk (be) minimised  
or controlled?**

**in order to adjust the risk level  
and assess the residual risk.**

For those risks assessed as Medium and High, the auditor will now examine management response in place. This examination allows the auditor to assess how well an entity is **managing major risks** rather than simply focusing on areas of suspected weakness. Risk response and **control activities** are the actions, policies and/or procedures that help to ensure that management directives are carried out, and that necessary actions are taken to address and reduce the risks to the achievement of the organisation's objectives. Several strategies can be adopted to deal with risk. **Risk can be avoided, reduced, tolerated, mitigated, eliminated or transferred.** Not all risks can or should be avoided; reducing all risk to "zero" is usually not cost-effective for the organisation.

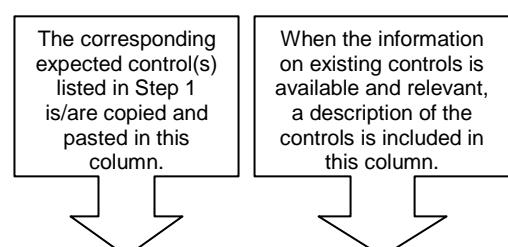
To identify the actions, controls and/or procedures that have been taken to counter the main risks identified, the auditor can start by taking the **List of Expected Key Controls** set up in the beginning of the risk assessment exercise and comparing these to the controls that management asserts to be in existence. It is also necessary to ascertain what **controls are actually in operation**, and **establish the extent of their limitations**. Controls can also be performed externally by, e.g., national certifying bodies or internally by the Internal Audit Service or a specific unit, e.g. a reconciliation unit.

Examples of controls may include:

1. Internal control systems as a whole and more specifically,
2. Financial controls
3. Segregation of duties, access controls, delegation of authorities
4. Policies and procedures for monitoring and supervision
5. Audit and evaluations
6. Reporting on performance and results
7. Guidelines, procedures, manuals, standard forms etc.
8. Training / information campaigns

The final assessment of the risk level, or **residual risk level**, takes into account the management response in place to adjust, i.e., increase or decrease the initial risk level, if appropriate. Reducing the risk level is a **critical decision that should be taken after careful consideration**, based on the experience and sound judgement of the auditor.

 Example of a Risk Analysis table adapted from the audit on the "Translation Expenditure of the Institutions".



The diagram consists of two boxes with arrows pointing to specific columns in the table. The left box contains the text: "The corresponding expected control(s) listed in Step 1 is/are copied and pasted in this column." The right box contains the text: "When the information on existing controls is available and relevant, a description of the controls is included in this column."

Area Objective Activity Process	Description of Risk cause + problem + impact	Likeli- hood H-M-L	Impact H-M-L	Risk level H-M-L	Expected key controls	Risk response	Residual Risk H-M-L
<b>3. Translation</b>							
3.1	<b>Risk of too much emphasis on quality</b> which would result in less productivity of translated documents	Low	Medium	M			
<b>4. Payment</b>							
4.1	<b>Risk of irregular procedures in the selection of freelancers and the assignment of jobs</b> due to non-compliance with the rules of the financial regulation. Each Institution recruited separately without any call for tender as annual amounts paid to individual freelancers were beneath the threshold. Irregular procedures constitute an infringement to the rules for which the Institution can be sued.	High	Medium	H	Controls ensuring that tendering procedures are compliant with Financial Regulation. Calls for tender ensuring that best value-for-money offers are selected.	Each Institution used to recruit separately without any call for tender as annual amounts paid to individual freelancers were beneath the threshold. Parliament and the Commission are now organizing joint tender for translation, which significantly reduces the likelihood of occurrence. =>Likelihood is adjusted to Low and risk level to Medium	M
4.2	<b>Risk of over - or under-payment</b> , i.e. that the correct price per page is not applied and that the deadlines for payments are not respected, due to insufficient controls, resulting in waste of money.	Low	Low	L			

## STEP ④ – FOCUS ON THE KEY RISKS TO DEFINE THE AUDIT QUESTIONS AND SCOPE

### Discuss and confirm the risk analysis with the auditee.

The risk assessment is now completed and the result is explained and documented in the Risk Analysis table. At this stage it is advisable to discuss and confirm the PLM, the flowchart and the risk analysis, with the auditee; then the auditor should formulate potential audit questions and focus the scope of the audit. To do so, (s)he should complete the **Potential Audit Questions & Scope – PAQS – table**.

### Prioritise the risks.

The risk assessment should identify matters of potential significance or issues for **in-depth audit**. Based on the level of risk/residual risk, the auditor should prioritise the risks to be able to single out and focus on the **key risks** i.e. risks which are significant and critical. Those will include all high-level risks and the medium-level risks that are considered critical. Typically, the matters which are the most critical to the success of the activity being audited, or those that present the greatest risks or opportunity for improvement, are proposed for detailed audit.

In most cases, risk assessments are based on more or less subjective judgements/qualitative information and there are no clear-cut answers to whether the risk is critical or not. The following elements can help the auditors in their decision:

#### Which of the risks identified are key risks to the audited area?

A risk should be considered as **critical**, if it can<sup>7</sup>:

- endanger or hamper the achievement of entity/policy/programme objectives.
- result in wasting significant amounts of money in the area under study.
- result in infringement of laws and regulations.
- result in material financial loss.
- put the safety of people or the environment at stake.
- cause serious damage to the EU's stakeholders and institutions.
- in any way seriously affect the EU's image and reputation.
- prevent objectives from being achieved according to the principles of economy, efficiency and effectiveness.

#### What audit question could address them?

Key risks can then be grouped in different ways, depending on the needs of the auditor and on the audit area, e.g. by process, objective, category (efficiency, effectiveness, economy). The auditor should then formulate potential audit questions to address one or several key risks. The questions can be formulated at a level of detail corresponding to a level-2 question of an Evidence Collection Plan.

#### Would an audit of any of the key risks add value?

Once the audit questions are set, to define the audit scope, the auditor must assess the potential relevance and interest of the audit question and its feasibility. Issues<sup>8</sup> to consider include:

1. the relevance and interest of the audit question:
  - a. the alignment of the audit subject with the European Court of Auditor's mandate
  - b. the financial significance (impact) of the risk or the amounts at stake. Figures can be obtained from, for e.g. the Financial Perspectives and from the level of budgetary commitments, final appropriations, cancellations and payments.
  - c. If there is any marked public interest, or a specific interest expressed by the Court, the discharge authority, another European Institution or the Member States.
  - d. If the conclusions of the audit can possibly influence the next regulatory framework or any important decision to be taken by the Commission or the Member States.
  - e. If there is any recent or parallel audit coverage or evaluation of the

#### Is it interesting and relevant enough to justify an audit?

7 Adapted from Risk Management in the Commission, European Commission, DG Budget, October 2010.

8 Further guidance on those criteria is given in the Performance Audit Manual, section 3.2.4 "Outline the audit".

topic, in which case the audit will have little added-value.

2. the feasibility of the replying to the audit question:

- a. risk for the European Court of Auditors to audit (auditability and feasibility) or not (credibility) this area. It is crucial to give a realistic assessment of the feasibility
- b. can the questions be answered?
- c. can a conclusion be reached in the light of the availability of the necessary information, audit methodologies, resources and audit skills?
- d. are conditions appropriate in terms of timing?

The PAQS table is filled in with the answers to these questions.

**Would such an approach be feasible?**

**Which audit questions should be included in the audit scope?**

With all the information displayed in the PAQS table, the auditor should now make a final proposal for whether or not to include the audit question in the scope of the audit.

Example of a PAQS table adapted from the audit on the "Translation Expenditure of the Institutions".

Area Objective Activity Process	Key Risk (all High level + critical Medium level risks)	Residual Risk level	Audit Question	Relevance & Interest H-M-L	Normal	Feasibility Difficult	To be include in Scope Yes-No
1. Request							
	<b>Risk of linguistic over-consumption</b> in case the authorisation procedures don't prevent applicants resorting to translation more often than absolutely necessary, e.g. translation of less important texts, translation when the individuals involved have a sufficient knowledge of the source language, which increases the costs. <b>(Economy)</b>	H	Do institutions have adequate procedures avoiding unauthorized and redundant translations?	High 3 693 781 total number of pages translated in 2001(100%)	Normal The documentation of the procedures in all services is very weak and there is almost no inventory of the documents in the institutions		YES
2. Planning							
	<b>Risk of inadequate distribution</b> of resources between institutions and units, due to the absence of interinstitutional cooperation, resulting in contracting freelancers when the same or another institution has available in-house capacity <b>(Efficiency)</b>	H	Is the distribution of resources between institutions and units adequately organized?	Medium	Difficult		YES
	<b>Risk of low productivity</b> because of uneven distribution of workload, inadequate management tools - translations are not finished in time, delaying meetings and court cases. <b>(Efficiency)</b>	M	Is the workload evenly spread out over the year?	High	Difficult The productivity of different translation services is very hard to compare because it depends on a large number of factors some of which beyond management control: e.g. tightness of the deadlines; the source language; computer tools; speed and application of each individual translator; time spent on terminology.		YES
3. Translation							
	<b>Risk of too much emphasis on quality</b> , i.e. unnecessary, time-consuming systematic revision, due to the lack of clear instructions by management, which would result in less productivity. <b>(Effectiveness)</b>	M	Do institutions have monitoring procedures to ensure that translations are delivered in due time and at the required quality?	Medium	Normal		YES
4. Payment							
	<b>Risk of irregular procedures</b> in the selection of freelancers and the assignment of jobs due to non-compliance with the rules of the financial regulation. Each Institution recruited separately without any call for tender as annual amounts paid to individual freelancers were beneath the threshold. Irregular procedures constitute an infringement to the rules for which the Institution can be sued.	M	Are the selection process and the assignment of jobs legal and equitable?	Medium 687 697 total number of pages by freelance translation in 2001(18,6%)	Difficult Often there is no written trace of the refusal of a job and will make it difficult to check if the ranking resulting from the tendering procedure was respected.		NO

## BIBLIOGRAPHY / SOURCES

<b>European Court of Auditors</b>	Performance Audit Manual of the Court, revised 2012. The internal working papers of the audit on the "Translation Expenditure of the Institutions" leading to ECA Special Report 09/2006.
<b>Commission</b>	Risk management in the Commission - Implementation guide, European Commission, DG Budget, Up-dated version October 2010.
<b>External documentation</b>	Enterprise Risk Management - Integrated Framework, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004. The Standards and Guidelines for the Professional Practice of Internal Auditing by the Institute of Internal Auditors (IIA). One Pass Planning, Office of the Auditor General of Canada. Internal Control management and evaluation tool, US GAO. Sawyer's Internal Auditing, 5 <sup>th</sup> edition. "The Practice of Modern Internal Auditing" IIA.
<b>Websites</b>	<a href="http://www.aicpa.org">www.aicpa.org</a> – Beyond traditional audit techniques <a href="http://www.coso.org">www.coso.org</a> <a href="http://www.mcneese.edu">www.mcneese.edu</a> – Audit manual 3200 Internal controls <a href="http://www.mindtools.com">www.mindtools.com</a> <a href="http://www.theiia.org">www.theiia.org</a> – Tone at the top <a href="http://www.wikipedia.com">www.wikipedia.com</a> on risk assessment

**Annex I - The Risk Assessment Process: input, tools and output.**

The risk assessment process is presented in the table below along with the **input, tools and output of each step of the process**.

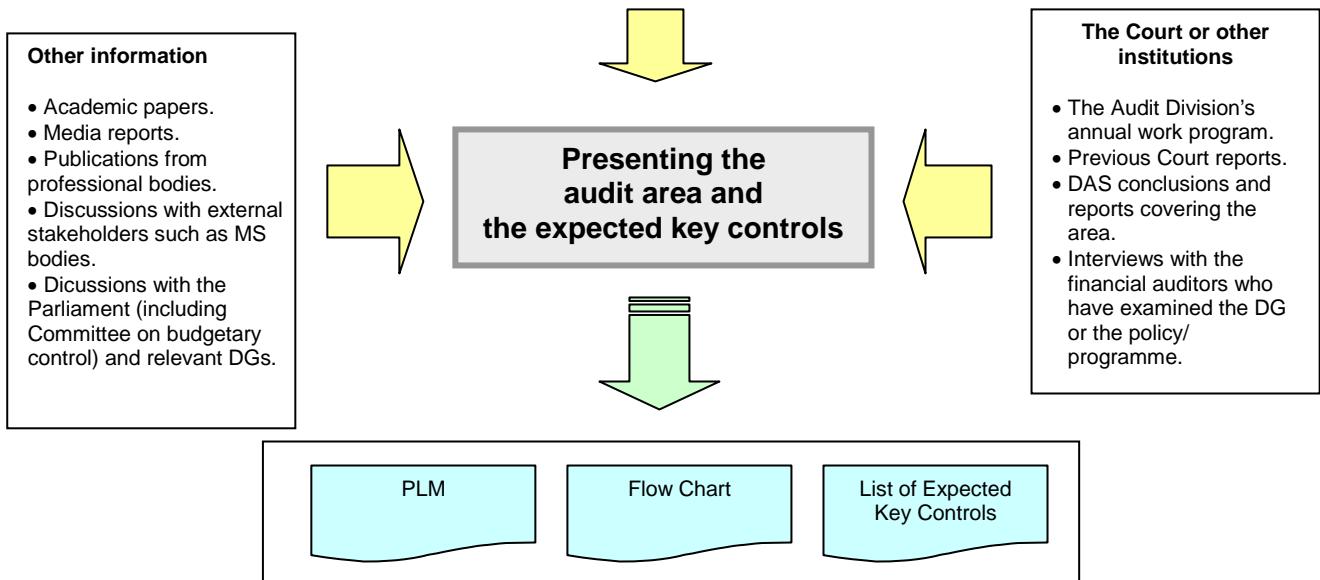
The table also gives the references to the Performance Audit Manual.

<b>Overview of the risk assessment process</b>					
Performance Audit Manual	Risk assessment step	Input	Tool	Output	Documentation in ASSYST One Working Paper
Ch.3 Par. 3.2.3	<b>Step 1: Present the audit area in a diagram &amp; list the expected key controls.</b>	Knowledge of the audit area.	- Sources of information (Annex II)  - Illustrative list of risk factors (Annex III).	<b>PLM and Flowchart</b> (p.6 and Annex II).  List of Expected Key Controls (p.7).	<a href="#">Risk_my audit.xls</a> template: 3 worksheets.  “PLM”, “Chart” and “Exp Key Cont”.
Ch.3 Par. 3.2.3	<b>Step 2: Identify the risks.</b>	PLM and Flowchart  List of Expected Key Controls.	Brainstorming.  How to describe a risk (p.8).  Examples of risks and risk categories (p.8 and annex IV).	<b>List of Identified Risks</b> (p.9).	<a href="#">Risk_my audit.xls</a> template: 1 worksheet.  “List of identified risks”.
	<b>Step 3: Analyse the risks to assess the risk level.</b>	List of Identified Risks.  List of Expected Key Controls	Risk matrix (p. 10)	<b>Risk Analysis table</b> (p. 12)	<a href="#">Risk_my audit.xls</a> template: 1 worksheet.  “Risk Analysis table”.
Ch.3 Par. 3.2.4	<b>Step 4: Focus on key risks to define the audit questions and scope.</b>	Risk Analysis table.	Sound judgement.	Potential Audit Questions and Scope - <b>PAQS table</b> . (p.15)	<a href="#">Risk_my audit.xls</a> template: 1 worksheet.  “PAQS table”.

## ANNEX II – Sources of information

### **Audited bodies**

- High level documents such as annual reports and business plans.
- Discussions with the auditee.
- Performance results compared with targets.
- Accounts.
- Risk self-assessment done by management.
- Work done by internal audit teams.
- Web pages.
- Reports from national Supreme Audit Institutions.
- Reports from Member States' Certifying Bodies.
- Rules and regulations, including implementing regulations and national instructions, the Financial Regulation, the Staff Regulation...
- EUROSTAT data.
- For audits involving the Commission :
  - the Annual Policy Strategy and annual Activity Statement,
  - the DG's Annual Management Plan and Annual Activity Report.
  - Evaluation reports and DGs evaluation plans and programmes.
  - Reports issued by the Clearance of Accounts unit.



**ANNEX III – Illustrative list of risk factors**

<b>Organisation</b>	<p><i>Structure</i></p> <ul style="list-style-type: none"> <li>◊ complex organisation (e.g. cross border operations, involving linguistic, political, or geographical issues, several administrative levels)</li> <li>◊ organisation often subject to structural changes</li> <li>◊ geographically dispersed organisation</li> <li>◊ decentralised management</li> </ul> <p><i>Resources</i></p> <ul style="list-style-type: none"> <li>◊ information technology that is obsolete, highly complex, or includes many different and/or incompatible computer systems</li> <li>◊ insufficient, under-qualified, inexperienced or poorly motivated staff and/or inadequate recruiting procedures</li> <li>◊ absence of common supporting administrative structure</li> <li>◊ IT systems when several services involved in managing the programme</li> <li>◊ large number of sub-contractors</li> <li>◊ employment of resources that are unnecessary, of too high quality, or that could have been obtained at lower cost</li> </ul> <p><i>Responsibilities</i></p> <ul style="list-style-type: none"> <li>◊ imposition of unwanted responsibilities upon organisations, administrations or beneficiaries</li> <li>◊ unclear division of responsibilities</li> <li>◊ lack of job descriptions</li> <li>◊ no policy for staff rotation</li> <li>◊ poor coordination of activities, especially in a decentralised or shared management system</li> </ul>
<b>Nature of the policy, programme and operations</b>	<p><i>Policy/programme</i></p> <ul style="list-style-type: none"> <li>◊ legal basis that is uncertain, complicated, or subject to significant change</li> <li>◊ significant degree of change in the environment of the programme</li> <li>◊ complex programme delivery method</li> <li>◊ complex contractual or tendering rules</li> <li>◊ rapid implementation of the programme after the decision on the legal base or, at the other extreme, slow implementation</li> <li>◊ no European added value / additionality - EU funds replace national government expenditure</li> <li>◊ poor sustainability (no ownership; projects set up without proper dialogue with beneficiaries; beneficiaries highly dependent on EU)</li> </ul> <p><i>Operations</i></p> <ul style="list-style-type: none"> <li>◊ large number of transactions</li> <li>◊ complex activities</li> <li>◊ activities involving large amounts of cash or high-value goods</li> <li>◊ activities with which the audited entity has no or limited experience</li> <li>◊ activities of a nature traditionally considered to be particularly prone to irregularities</li> <li>◊ urgent operations</li> <li>◊ new initiatives set up in haste</li> <li>◊ activities funded by other sources (other EU instruments or co-financing)</li> <li>◊ contracts frequently awarded without competition</li> <li>◊ high proportion of commitments or payments made late in the financial year</li> <li>◊ difficulty in identifying final beneficiary</li> </ul>
<b>Objectives</b>	<p><i>Objective-setting</i></p> <ul style="list-style-type: none"> <li>◊ inadequate assessment of needs</li> <li>◊ lack of, unclear, inadequate or unquantified objectives regarding economy, efficiency and effectiveness</li> <li>◊ objectives do not include legality, regularity, accuracy and reliability of accounts, safeguarding of assets</li> <li>◊ objectives not prioritised, or priorities unclear</li> <li>◊ objectives contradictory or incompatible, either in the EU policy or programme, or between EU and national priorities</li> <li>◊ objectives not communicated to all levels of management</li> </ul> <p><i>Operationalising the objectives</i></p> <ul style="list-style-type: none"> <li>◊ no clear link between objectives and activities</li> <li>◊ eligibility/selection criteria unclear or inconsistent with objectives (too wide, too restrictive or not relevant)</li> <li>◊ critical factors that could endanger achievement of objectives not regularly assessed</li> </ul>

<b>Performance measurement</b>	<p><i>Use of performance indicators</i></p> <ul style="list-style-type: none"> <li>◊ lack of indicators to measure achievement of economy, efficiency, and effectiveness</li> <li>◊ use of indicators that are inappropriate, or that may encourage the wrong behaviour (e.g. pursuit of short-term goals to the exclusion of long-term goals)</li> </ul> <p><i>Measuring and monitoring performance</i></p> <ul style="list-style-type: none"> <li>◊ lack of a system to monitor actual performance against plan</li> <li>◊ evidence of poor performance, as indicated by, for example: <ul style="list-style-type: none"> <li>- high level of complaints</li> <li>- low level of user satisfaction</li> <li>- disparities in performance with other organisations, or among beneficiaries</li> <li>- poor performance of contracted-out services</li> </ul> </li> </ul>
<b>Management</b>	<p><i>Ethical issues</i></p> <ul style="list-style-type: none"> <li>◊ ethical values/integrity poorly established (tolerance towards irregularities, no code of conduct)</li> <li>◊ strong pressure on management to achieve unrealistic objectives or meet unrealistic deadlines (e.g. high rate of commitment of budget appropriations)</li> <li>◊ political or other pressures on management to perform in a particular way</li> </ul> <p><i>Management performance</i></p> <ul style="list-style-type: none"> <li>◊ evidence of poor management, as indicated by, for example: <ul style="list-style-type: none"> <li>- past records of mismanagement in the area/countries</li> <li>- significant cost and time overruns on projects</li> <li>- inadequate planning</li> <li>- lack of supervision and monitoring</li> </ul> </li> </ul> <p><i>Management information</i></p> <ul style="list-style-type: none"> <li>◊ lack of, or inappropriate, management information system</li> <li>◊ management and financial information poor, not used or used inappropriately</li> </ul>
<b>Controls</b>	<p><i>Control systems</i></p> <ul style="list-style-type: none"> <li>◊ lack of internal control systems to monitor economy, efficiency and effectiveness</li> <li>◊ weaknesses in the design or performance of control systems</li> <li>◊ complex control systems</li> <li>◊ supervision and control functions non-existent or unsuitable</li> <li>◊ differences in the control systems amongst beneficiaries/Member States</li> <li>◊ operations not fully subject to the usual controls</li> <li>◊ on-the-spot inspection or monitoring rights not taken up or infrequently used</li> </ul> <p><i>Financial controls</i></p> <ul style="list-style-type: none"> <li>◊ beneficiaries' accounting systems incompatible with the Community systems</li> <li>◊ excessive costs in the programme, or expenditure increasing beyond expectations</li> <li>◊ difficult to determine the cost of inputs</li> <li>◊ budget targets that are consistently missed to a significant degree</li> <li>◊ lack of a cost accounting system</li> </ul> <p><i>Audit and evaluation</i></p> <ul style="list-style-type: none"> <li>◊ inadequate audit system (coverage, quality, reporting, follow-up)</li> <li>◊ past issues as regards economy, efficiency and effectiveness, and/or legality and regularity</li> <li>◊ past audit findings not implemented</li> <li>◊ lack of, or poor, evaluation, and/or no follow-up of evaluation results.</li> </ul>

\*\*\*

## ANNEX IV – Examples of risks

### 1 – THE EUROPEAN COURT OF AUDITORS: EXAMPLES OF CONTROL RISKS.

Category	Control Risk
ECONOMY	<p>The risk that the Commission or the Member State(s) (MS) do not apply the principle of economy:</p> <ul style="list-style-type: none"> <li>• as they have no adequate mechanism to monitor that the desired outcomes are being achieved at the minimum cost.</li> <li>• because the procedures in place do not ensure that costs are the lowest available.</li> </ul>
EFFICIENCY	<p>The risk that the programme is not managed efficiently because :</p> <ul style="list-style-type: none"> <li>• Commission or the MS do not consider and monitor the costs compared with the benefits received.</li> <li>• The Commission or the MS have inadequate procedures to prioritise and select projects to ensure the maximum impact from Community funds.</li> <li>• The Commission does not cooperate with the delegated bodies to ensure timely implementation of financial and technical cooperation projects and reduction of costs.</li> </ul>
EFFECTIVENESS	<p>The risk that the programme is not effective as:</p> <ul style="list-style-type: none"> <li>• there is no mechanism in place to ensure that activities financed are in line with the quantitative financial objective of the EU.</li> <li>• the Commission and MS have not set up and properly implemented suitable measures to monitor the impact of the policy.</li> <li>• the Commission and MS have not carried out an adequate assessment of needs and possible benefits arising from the programme to support the funding decisions.</li> <li>• the Commission and MS have not set up and properly implemented appropriate mechanism to identify weaknesses and deviation from the objectives.</li> <li>• the procedures put in place by the Commission and MS are not appropriate and properly implemented.</li> <li>• there is an incoherent management within the Commission's services: different objectives and key performance indicators.</li> <li>• different key performance indicators are used by the Commission and the MS.</li> </ul>

### 2 – THE EUROPEAN COMMISSION'S RISK CATEGORIES: EXAMPLES OF RISKS.

Main risk categories		Examples of risks
External environment (outside DG/Commission)	External environment (outside DG/Commission)	<p>1. <b>Macro environmental</b> risks</p> <ul style="list-style-type: none"> <li>• Humanitarian aid does not reach the dedicated population due to corruption/social instability/armed conflicts</li> </ul> <p>2 Risks related to <b>political decisions</b> and priorities taken outside the Commission (e.g. other EU Institutions, MS)</p> <ul style="list-style-type: none"> <li>• Commission's objectives impacted by low political support in Member States.</li> <li>• Delays in programme delivery due to complex or changing environment</li> </ul> <p>3 Risks related to <b>external partners</b> (e.g. agencies, outsourcing, consultants, media)</p> <ul style="list-style-type: none"> <li>• Delays in the implementation of a specific programme due to poor performance by service provider/contractor.</li> </ul>
Internal	Planning, processes and systems	<p>1 Risks related to <b>strategy, planning and policy</b>, including internal political decisions</p> <ul style="list-style-type: none"> <li>• Performance affected by unclear strategies or objectives</li> <li>• Expectation gaps caused by the absence of agreed objectives and performance targets</li> </ul> <p>2 Risks related to <b>operational processes</b></p> <ul style="list-style-type: none"> <li>• Difficulties in implementing new policies caused by lack of adequate legal instruments</li> <li>• Ineffective implementation of programs caused by cumbersome operational procedures</li> </ul> <p>3 Risks related to <b>financial processes and budget allocation</b></p> <ul style="list-style-type: none"> <li>• Payment of ineligible costs caused by unclear financial rules</li> <li>• Incoherence between objectives and available budget (unbalanced budget)</li> </ul> <p>4 Risks related to <b>IT and other support systems</b></p> <ul style="list-style-type: none"> <li>• Operational performance affected by obsolete IT systems</li> </ul>
	People and the Organisation	<p>1 Risks related to <b>human resources</b> (staffing, competences, collaboration):</p> <ul style="list-style-type: none"> <li>• Implementation delays and errors caused by a lack of competence and expertise</li> </ul> <p>2 Risks related to <b>ethics and organisational behaviour</b> (e.g. "tone at the top", fraud, conflicts of interests, , reference made e.g. to ECA special report 15/2012 – Management of COI in EU agencies)</p> <ul style="list-style-type: none"> <li>• Adverse reputation and financial loss due to conflicts of interest (e.g. discriminatory usage of contractors)</li> <li>• Fraud or irregularities caused by a lax attitude towards rules and regulations</li> </ul> <p>3 Risks related to the <b>internal organisation</b>:</p> <ul style="list-style-type: none"> <li>• Operational performance affected by insufficient supervision arrangements</li> <li>• Delayed or ineffective decision making due to insufficient/inappropriate delegation of authority.</li> <li>• Frauds/irregularities due to absence of segregation of duties</li> <li>• Inefficiencies due to absence of clear reporting lines</li> </ul> <p>4 Risks related to the <b>security</b> of staff, buildings and equipment:</p> <ul style="list-style-type: none"> <li>• Theft of high-value equipment or sensitive information caused by insufficient access control to premises</li> </ul>

