EUROPEAN COMMISSION
Budget

Central Financial Service

Risk Management in the Commission

Implementation Guide

Updated Version - October 2010

TABLE OF CONTENTS

INTRODUCTION **3**

1. DEFINITIONS AND CONCEPTS **4**

1.1. WHAT IS A RISK? 4
1.2. WHAT IS RISK MANAGEMENT? 4
1.3. HOW DOES RISK MANAGEMENT ADD VALUE? 5
1.4. WHO SHOULD PERFORM RISK MANAGEMENT? 5
1.5. RISK MANAGEMENT AND THE INTERNAL CONTROL STANDARDS FOR EFFECTIVE MANAGEMENT ... 6
1.6. RISK MANAGEMENT AND THE SPP CYCLE 6

2. THE KEY STEPS IN THE RISK MANAGEMENT PROCESS **8**

2.1. STATING ACTIVITIES AND RELATED OBJECTIVES 8
2.2. IDENTIFYING AND ASSESSING THE RISKS 8
2.2.1. Identify the risks 8
2.2.2. Prioritise the risks (identify "critical" risks) 10
2.2.3. Cross-cutting risks 10
2.2.4. Documenting risks in risk register 11
2.3. DECIDING HOW TO DEAL WITH THE IDENTIFIED RISKS ("RISK RESPONSE") 11
2.4. IMPLEMENTATION OF THE RISK RESPONSE (ACTION PLANS) 14
2.5. MONITORING AND REPORTING 14

3. RISK MANAGEMENT IN PRACTICE **15**

3.1. PLANNING AND ORGANISATION 15
3.1.1. Skills and awareness 15
3.1.2. Coordination 15
3.1.3. Timing/Agenda 16
3.1.4. Communication to participants 17
3.1.5. Scope and approach 17
3.1.6. Stating activities and related objectives 18
3.2. RISK IDENTIFICATION AND ASSESSMENT 19
3.2.1. Risk identification 19
3.2.2. The role of external partners in the risk identification process 22
3.2.3. Risk assessment 22
3.2.4. Critical risks 24
3.2.5. Cross-cutting risks 25
3.2.6. Risk inter-dependencies 25
3.3. REPORTING AND ACTION PLANS 27
3.3.1. Special case - risks outside management's control 27
3.3.2. Risk registers 28
3.3.3. Action plans 28
3.3.4. Contingency plans for accepted critical risks 29
3.4. SPECIFIC RISK REVIEWS (NOT DIRECTLY LINKED TO THE MP) 30

ANNEX 1 - RISK TYPOLOGY **32**

ANNEX 2 - RISK ASSESSMENT **34**

ANNEX 3 - RISK REGISTER **36**

ANNEX 4 - GENERIC QUESTIONNAIRE FOR RISK IDENTIFICATION AND ASSESSMENT ... **37**

GLOSSARY **46**

CONTACTS AND REFERENCES **47**

INTRODUCTION

Purpose and Context

In recent years, many organisations - both public and private - have implemented structured Risk Management in order to improve strategic decision making, increase operational effectiveness and set up risk-based Internal Control arrangements (better controls in some areas, less control in others where risk is assessed as being lower).

The specific framework, common vocabulary and basic principles for Risk Management were adopted by the Commission in October 2005[1]. Risk Management is also governed by Internal Control Standard 6 (ICS 6), in which Risk Management was further strengthened in comparison with the previous standards and the basic Risk Management principles (adapting controls to risks identified) applied to all the revised standards. Moreover, Standard 6 (Risk Management process) refers specifically to the process in place for identifying risks in the annual planning phase, in conformity with the principles laid down in the common Risk Management methodology as defined in the Communication[2].

As far as financial management is concerned, the Authorising Officer by Delegation must put in place management and control procedures which take account of risks (article 60§4 of the Financial Regulation[3]).

The Approach

The Commission's Risk Management approach is strongly inspired by the internationally recognised COSO Enterprise Risk Management framework[4]. It has however been adapted to fit the Commission's activities and specific working environment. Basically, the idea is to perform a structured and continuous identification of the DGs' most significant risks and make sure these are managed in line with management's "acceptable risk level". This concept is explained in section 2.

The Implementation Guide

This **revised** guide takes into account the recommendations of the Internal Audit Service following their audit and survey on Risk Management in the Commission[5], two workshops organised with ICCs in April 2010, a discussion in the Group of Resource Directors (GDR) in June 2010 and other feedback provided by the DGs. It replaces all previous versions of the Guide.

[1] Communication to the Commission from Ms GRYBAUSKAITÉ in agreement with the President and vice-President Kallas “Towards an effective and coherent Risk Management in the Commission services” of 20 October 2005 (SEC(2005)1327).

[2] Communication to the Commission from Ms GRYBAUSKAITÉ in agreement with the President and vice-President Kallas “Towards an effective and coherent Risk Management in the Commission services” of 20 October 2005 (SEC(2005)1327).

[3] Article 60§4 of the Financial Regulation

[4] COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (known as the "Treadway Commission"). The Committee of Sponsoring Organisations of the Treadway Commission (COSO) issued at the beginning of the nineties an Internal Control Integrated Framework.

[5] Final Report ARES/IAS (2010)36631.

In addition to the guide, more specific guidance for Risk Management exists in the area of IT management. Guidance for grant management, legislative initiatives and agencies aspects will be provided in the future.

1. DEFINITIONS AND CONCEPTS

1.1. What is a risk?

In the Commission, a risk is defined as "*Any event or issue that could occur and adversely impact the achievement of the Commission's political, strategic and operational objective. Lost opportunities are also considered as risks*".

Hence, risks relate to the non-achievement of objectives. Whereas many risks are associated with the DG's performance objectives (i.e. to the effective and efficient achievement of political and operational objectives[6]), others relate to compliance objectives (for example the legality and regularity of activities and financial transactions) or 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 Commission 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 Commission 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.

> **Example:** the risk of inadequate translation might be accepted depending on the circumstances and the type of document. If the document is not going to be legally binding, and is intended for internal use only, and thus errors in translation will not have a financial or legal impact, the document will be equally understandable for the users and interpreted in the same way, a mistake in translation may exceptionally be accepted, assuming of course that the mistake was detected ex-post, that its correction will be time-consuming and that it has almost no impact on the practical application of the document.

[6] *for the definition of the policy, strategic and operational objectives refer to the Standing Instructions for the establishment of the MP*

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. Regardless of the domain, the same basic questions apply: considering the risks involved, are the current controls or measures taken relevant and do they reduce risk sufficiently? Should they be simplified or further developed?

To a large extent, **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 guide 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 a service'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 senior management level:* a structured and consistent management approach facilitates the coordination, analysis and management of risks at overall Directorate or DG level. It is also necessary for the effective management of cross-cutting risks affecting several DGs and, when appropriate, Executive Agencies or external bodies;

- *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;
  - 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 **Director General** is ultimately responsible for the management of the DG's activities and achievement of objectives and must ensure that the DG's critical risks are known and appropriately managed. This role includes "setting the tone" for

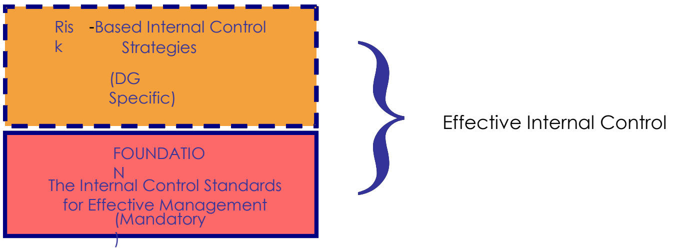
Risk Management, sponsoring Risk Management exercises, assigning responsibilities and reaching a view on the treatment of critical risks;

- **Managers and members of staff** as the experts are responsible for managing risks related to their main activities and objectives;
- The **Internal Control Coordinator** (ICC) supports managers in setting up a coherent and effective Risk Management process in the DG. The role involves facilitation, support and monitoring rather than directly managing risks per se and the ICC may be assisted in this by one or more dedicated staff under his/her authority or by a specific Rsk Management working group. A model Job Description of the ICC is presented on BudgWeb, which may be adapted as necessary to fit DGs' own circumstances;
- **Internal auditors** (IAC/IAS) perform independent regular assessments and make recommendations for improving the effectiveness of Risk Management, control and governance processes. The mission and objectives of the IAC and the IAS are presented in detail respectively in the model Charter of the Internal Audit Capability and in the Internal Audit Service Charter;
- The **Commissioner** is kept informed of critical risks affecting his/her DG(s) via the MP process and via the regular (at least half-yearly) updates on Internal Control, as required by ICS9.

1.5. Risk Management and the Internal Control Standards for Effective Management

Risk Management is part of effective Internal Control. Whereas the 16 Internal Control Standards for Effective Management (ICS) constitute the basic management principles (regardless of the DG's working environment and activities), Risk Management facilitates the establishment of DG-specific Internal Control environment 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.

Diagram 1 - Risk Management and the ICS


Ris
k -Based Internal Control
Strategies
(DG
Specific)
FOUNDATIO
N
The Internal Control Standards
for Effective Management
(Mandatory
)
Effective Internal Control

1.6. Risk Management and the SPP cycle

To be effective, Risk Management must be part of everyday management (with the level of action dependent on the level of risk involved). In practical terms, Risk Management should be fully integrated into the different steps in the SPP-cycle:

- the planning and programming phase (which is the main focus of this document);
- during the execution phase (follow-up on Risk Management implementation plan and specific risk reviews of processes/projects/systems - see section 3.4);
- and as part of the reporting (AAR and intermediate reporting).

Performance indicators, defined as part of the MP-based Risk Management process, should be monitored regularly in order to allow early identification of emerging threats that may impair the achievement of objectives.

Although such regular monitoring may take the form of an informal exercise, a quarterly formalisation of the conclusions is recommended for the most significant risks. At least twice per year, at the moment of the adoption of the Management Plan and at the moment of the mid-term review, formalisation is mandatory.

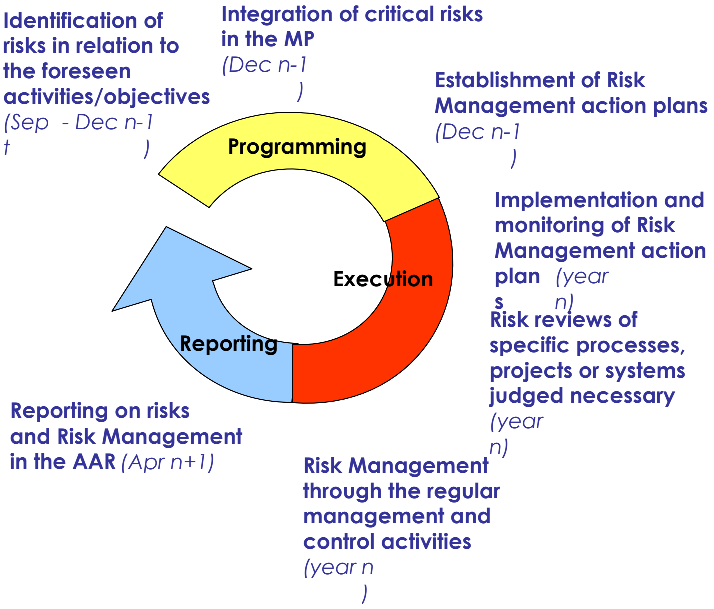
NEW!

To ensure readiness to react to new or changed risks and threats, Risk Management is a **continuous exercise**. Therefore DGs 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 DG/the Commission
- staff changes in crucial positions (particularly key management and specialist staff)
- external events e.g. financial crisis, threat of pandemic, natural disaster.
- new legislation for the DG's operations
- failure of Risk Management as regards critical risks

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

Diagram 2 - Risk Management and the SPP-cycle

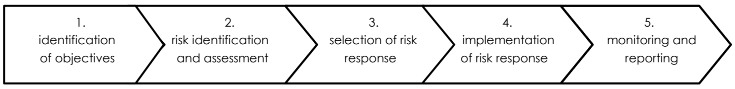

Identification of risks in relation to the foreseen activities/objectives (Sep t - Dec n-1)
Integration of critical risks in the MP (Dec n-1)
Establishment of Risk Management action plans (Dec n-1)
Programming
Execution
Reporting
Implementation and monitoring of Risk Management action plans (year n)
Risk reviews of specific processes, projects or systems judged necessary (year n)
Reporting on risks and Risk Management in the AAR (Apr n+1)
Risk Management through the regular management and control activities (year n)

The diagram presents the position of Risk Management in the SPP-cycle at the level of the Commission. However, Directorates-General are encouraged to introduce Risk Management as a continuous exercise as explained in the frame above.

2. THE KEY STEPS IN THE RISK MANAGEMENT PROCESS

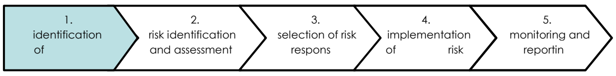
The Risk Management process is divided into five steps, as shown in the following diagram:

Diagram 3 - The five steps of the Risk Management process


1. identification of objectives
2. risk identification and assessment
3. selection of risk response
4. implementation of risk response
5. monitoring and reporting

2.1. Stating activities and related objectives

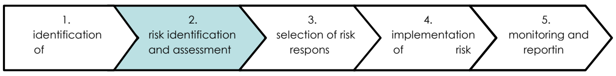
What is the purpose of the DG's activities? What should be achieved?


1. identification of
2. risk identification and assessment
3. selection of risk respons
4. implementation of risk
5. monitoring and reportin

- *Clearly stating activities and related objectives* in the Management Plan 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?


1. identification of
2. risk identification and assessment
3. selection of risk respons
4. implementation of risk
5. monitoring and reportin

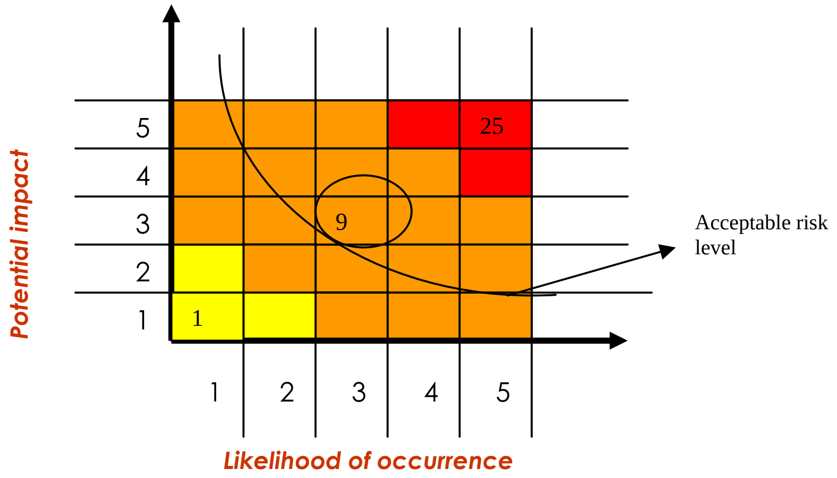
2.2.1. Identify the risks

- *Taking into account all aspects when identifying risks:* there are many types of risks, both internal and external, depending on the specific nature of activities. The Commission's Risk Typology (see annex 1) sorts these into groups and it should be used to ensure that the most common risk aspects are covered. Any difficulty in using the typology should be raised with Unit BUDG D3 (e-mail to BUDG-mailbox-xxx@xx.xxxxxx.xx);
- *Formulating the risks clearly:* before assessing a risk, it must be clearly explained: (1) How would it impact the DG'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). The **risk map** (see Diagram 4) is a graphical presentation of the impact and likelihood and is a widely used tool to prioritise risks and highlight those which could significantly impact on the ability to accomplish the objectives. On the risk map, the impact is plotted on the vertical axis and the likelihood on the horizontal axis. The more a risk is located to the top-right corner, the higher the risk level.

This assessment of risks is further explained in Annex 2.

Diagram 4 - The Impact/Likelihood model



Residual vs. inherent risk: Management should be aware that **residual** (not inherent) risks are subject to risk assessment. **Inherent** risk is the risk related to the very nature of the organisation's activities e.g. the risk of pandemic for DG SANCO. **Residual** risk is the assessed level of risk remaining after the controls put 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.

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

Determining if any risks are "critical": in line with SEC(2005)1327, a risk should be considered "critical" and reported in the MP (Management Plan) if it can:

(a) jeopardise the realisation of major policy objectives[7];

(b) cause serious damage to the Commission's partners (Member States, companies, citizens, etc.);

(c) result in critical intervention at political level (Council/Parliament) regarding the Commission's performance;

(d) result in the infringement of laws and regulations;

(e) result in material financial loss;

(f) put the safety of the Commission's staff at risk; or

(g) in any way seriously damage the Commission's image and reputation.

(h) even if not covered by the above categories, a risk could also be considered as "critical" if the combination of its impact and likelihood falls in the upper end of the scale as presented in Diagram 4. Because of the different acceptable risk levels, it is up to the DG to define the threshold (as per Diagram 4) for a particular risk to be critical. The threshold for critical risks does not have to be equivalent to acceptable risk level - the latter being rather the level of risk necessitating reaction.

2.2.3. Cross-cutting risks

Risks are considered cross-cutting if:

- they affect several Services; and
- they can be evaluated or addressed more effectively by a group of Services rather than by an individual service.

A structure which facilitates the analysis and management of cross-cutting risks has been developed by the central services since 2007. The Procedure for managing cross-cutting risk is available on BudgWeb.

Central in this procedure is the **notification to SG and DG BUDG** of potential cross-cutting risks using a "notification template". The objective of this notification is to ensure the appropriate follow up to critical cross-cutting risks at Commission-wide level. As of 2009, the timing of the notification of cross-cutting risks is aligned with the timing for submission of the draft MPs. Where judged appropriate by the central services, the DGs concerned are invited to discuss notified cross-cutting risks in a "peer review". In all cases, the central services provide feedback on the cross-cutting risk notification to the notifying DG and maintain a central list of cross-cutting risks.

Risks that affect several Services but can be appropriately evaluated and addressed by one service should NOT be notified to the Central Services (and therefore are not subject to a peer review). In this case, it is the responsibility of the concerned DG to ensure that the risk is assessed and managed jointly with other DGs.

[7] *for the definition of the policy, strategic and operational objectives refer to the Standing Instructions for the establishment of the MP*

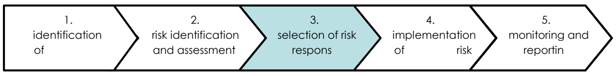
2.2.4. *Documenting risks in risk register*

NEW!

Documenting the most significant risks in a risk register: to make the exercise focussed and manageable, the most significant risks must be singled out and documented in a risk register to provide a record of risks and the measures taken to manage them. It is required that each DG keeps one regularly updated risk register containing the most significant risks at DG-level, for example under the authority of the Internal Control Coordinator. The **minimum mandatory** content of the risk register is presented in Annex 3. Depending on the size of the service and the complexity of the risk environment, it may also be useful to keep risk registers at Directorate and Unit levels. In such cases, DGs must ensure that critical risks are documented in the central risk register.

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

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


1. identification of
2. risk identification and assessment
3. selection of risk respons
4. implementation of risk
5. monitoring and reportin

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

NEW!

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 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); - this response is the most difficult to implement in the case of the Commission which has strategic objectives derived from the Treaty, legislation and the Budget;

(2) **Transfer** them to/**share** them with third parties (for example by outsourcing or using an insurance company). Again such transfers are relatively rare in Commission terms;

(3) **Reduce** the risks (for example by improving controls or taking other relevant action) - 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) or **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 **risk level** (the combination of impact and likelihood). Whereas it's 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.

The four possible risk responses are illustrated with examples below. This is only an indicative illustration - selecting the right risk response is each time a matter of subjective judgement and Management decision.

Risk description	Risk level	Risk Response
Due to a lack of registered candidates one month before a training course, there is a risk that the course will not take place. For all the cancellations done later than two weeks before the training, 50% of the trainer's fee needs to be paid in compensation.	**Low** (In quantifiable terms equal to 50% of the daily rate of a trainer)	**Avoid** (Better to discontinue this activity i.e. cancel the training, than to incur the compensation costs)

Risk description	Risk level	Risk Response
Due to recruitment issues and lack of staff, there is a risk that the contractor will not deliver a study ordered by the Commission to the required standard or within the deadline, which will put the realisation of one of the Commission's key projects at risk.	**High**	**Transfer** (The performance guarantee - the clause in the contract which says that the contractor incurs the costs in case the final product does not meet the requirements of the Commission)

Risk description	Risk level	Risk Response
Due to a temporary lack of interpreters in certain EU languages (BG, RO), there is a risk that a high-level conference will need to be cancelled, which might have impact on the reputation of the Commission.	**High**	**Reduce** (Consider contracting with freelance interpreters)

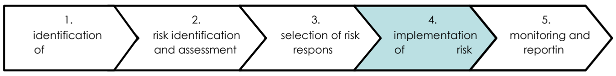
Risk description	Risk level	Risk Response
As a result of refurbishment, several training rooms will not be available during summer holiday period, with the consequence that training sessions will need to be postponed. The work is however due to be completed beforehand and the contractor has a good delivery record.	**Low**	**Accept**

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:* this is the total impact of risk an organisation is prepared to accept in the pursuit of its strategic objectives. DGs are invited to define their acceptable risk levels for quantifiable as well as for unquantifiable risks:
- *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**. Should a tolerable risk of error level have been decided by the Legislative Authority, this level may be used as a reference but it should be borne in mind that such levels would be fixed for a policy area or group of DGs and that risk profiles of the different activities within this group will be likely to differ significantly. In all cases therefore 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)

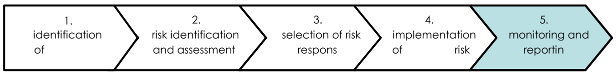
What concrete actions are needed to address the risks?


1. identification of
2. risk identification and assessment
3. selection of risk respons
4. implementation of risk
5. monitoring and reportin

- *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 (what is the underlying problem?). 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. They should be documented, and those which are most important logged in the central risk register, the minimum mandatory content of which is set out in Annex 3.

2.5. Monitoring and reporting

Do the action plans remain relevant and effective?


1. identification of
2. risk identification and assessment
3. selection of risk respons
4. implementation of risk
5. monitoring and reportin

- *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 ICC for the most important risks;
- *Reporting on implementation of action plans is done in the Annual Activity Report.* While the Annual Activity Report is destined to be published and should not include sensitive information, it should provide information of key activities including how the overall risk levels have been managed. Detailed instructions can be found in the Standing Instructions for Annual Activity Reports on BudgWeb.

3. Risk Management in practice

Whereas the previous chapter introduces the general Risk Management principles, this chapter focuses on practical implementation.

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 (Syslog*): DG BUDG/HR offer three Risk Management courses via Syslog: (1) Risk Management for **Managers**, (2) Risk Management for **ICCs** and (3) Risk Management for **Staff**. Whereas the first course focuses on Risk Management from a Unit Head's perspective, the aim of the second one is to provide advice for organising and coordinating Risk Management exercises in a DG. Risk Management for Staff is a half-day session providing some basic information on Risk Management concept to all staff. Exchange of experiences and good practices are key elements in all the courses;
- *Risk Management training (DG internal)*: In the past, certain DGs have organised their own Risk Management training sessions internally. The advantage is that these can be tailored to the DG's specific working environment and activities. A framework contract is available for this purpose (contact BUDG-10-PO-CI);
- *Risk Management seminars:* organising Risk Management seminars can be an effective way of raising management's and staff's awareness. The framework contract mentioned above can also be used for this purpose. The ICC can also animate general or targeted risk assessment exercises;
- *BUDGWEB*: a range of useful information regarding Risk Management is available on http://www.cc.cec/budg/man/icrm/rm/rm_en.html
and
http://www.cc.cec/budg/man/icrm/services/guidelines/rmguidelines_en.html

3.1.2. Coordination

- *Flexibility*: the Risk Management exercise can be coordinated in different ways. The annual exercise should be fully integrated into the MP process, while at the same time ensuring its continuous nature to facilitate reaction to a changing risk environment. In general, the Internal Control Coordinator (ICC) 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. To support the ICC, a specific Risk Management group/facilitation team can be set up, for example including persons from the MP-team, the IAC and other relevant staff. The facilitator role of the ICC is broadly defined in the model Job Description of the ICC available on BudgWeb;

- *IAC's role*: the general role of the IACs is defined in SEC(2003)59. Information about the IAC's role in Risk Management is provided in the Model Charter of the Internal Audit Capability: "The IAC helps the DG accomplish its objectives by bringing a systematic, disciplined approach in order to evaluate and make recommendations for improving the effectiveness of Risk Management, control, and governance processes[8]… Consulting Services are advisory and management-requested activities, (…) which are intended to add value and improve DG's governance, Risk Management, and control processes without the internal auditor assuming management responsibility." (…) The primary objective of the IAC is to provide the Director General with assurance as to the effectiveness and efficiency of Risk Management, control, and internal governance processes in the DG …" We recommend that ICC and IAC work closely together, co-ordinate their assurance exercises and share information about risks and the control environment of the organisation;

- *Documenting Roles and Responsibilities*: to ensure clarity and promote understanding within the DG, we recommend documenting the main roles and responsibilities related to the organisation and coordination of the Risk Management exercise.

3.1.3. Timing/Agenda

- *The MP process:* Each year in the first part-session of September (n-1), a State of the Union debate is held in which the President of the Commission delivers an address which sets out the priorities for the following year. In parallel, the President sets out in writing the main elements guiding the preparation of the Work Programme for the following year. This Work Programme is then adopted by the Commission in October (n-1) following exchanges of view with the Council and the European Parliament. The DGs prepare their **Management Plans (MP**) in parallel to this. Since Risk Management is integrated into the MP-process, annual risk management exercises are in this period: ideally, the **planning** of the exercise should start **already in July-September**;

- *Required time:* depending on the complexity of activities and scope (see 3.1.5), the Risk Management exercise linked to the MP can generally be carried out in 2-6 weeks provided it is well planned;

- *A continuous exercise*: note that Risk Management should be carried out continuously to facilitate reaction to changes in risk levels. This does not involve extensive new actions but rather a review by the responsible managers to identify and new or changed risks which should be assessed. In addition to the Risk Management exercise linked to the MP, there should be regular updates of critical risks, and, if judged necessary, specific risk reviews of processes/projects/systems during the year (see section 3.4) - for example in the light of changes in the organisation, policy or activity in question;

3.1.4. Communication to participants

- *Involve top-management:* to be effective, the Risk Management exercise **requires strong top-management involvement**. Workshops, seminars and similar events can be organised to raise management's awareness of the Risk Management concept. Ideally,

[8] Including promoting appropriate ethics and values within the organisation, ensuring effective organisational performance management and accountability, effectively communicating risk and control information to appropriate areas of the organisation, via established lines of responsibility.

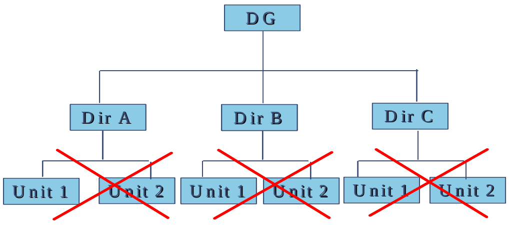
the Risk Management exercise should be announced and sponsored by the Director General;

- *Presentations:* we recommend organising presentations or workshops at Directorate and/or 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. A presentation template, which can be adapted to the DG's needs, is available.

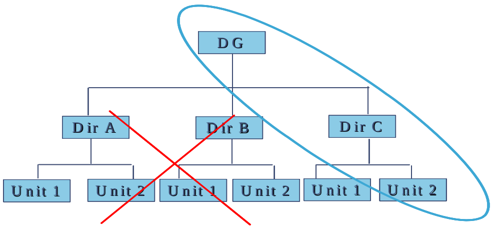
3.1.5. *Scope and approach*

- *Top-management steer*: top-management should steer the Risk Management exercise. This is primarily done by defining the scope, i.e. deciding what the MP Risk Management exercise should cover and deciding if there is a need to perform additional risk reviews of processes/projects/systems during the year (see section 3.4);
- *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 (risk identification by Directors) may be used to identify activities or areas where a more detailed review is necessary (targeted review). Depending on the size of the organisation, a risk steering committee advising the Director-General in terms of monitoring the risk management process and in terms of quality review of the most significant risks could be established;
- *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. Targeted reviews are described in details in section 3.4;
- *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.

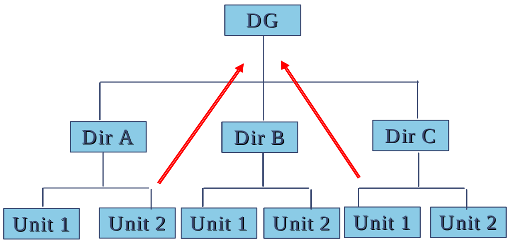
Diagram 5: The coverage of the Risk Management exercise



High level review: High-level reviews (risk identification by Directors) covering all main activities and related objectives at Directorate level are sometimes carried out to identify areas or activities where more detailed risk reviews should be carried out (targeted reviews).



Targeted review: Top-management wants to focus the exercise on a few specific domains or activities. Activities considered very stable and whose risks are well-known are not covered.
Top-management may also steer the exercise by building the exercise around "risk themes" instead of activities.



Bottom-up perspective: The Units inform top-management on how they perceive their main risks. An extensive bottom-up review covers all Units' main activities and related objectives.

	High level review	Targeted review:	Bottom-up perspective
Context	• Top-management in regular contact with all the levels in organisation • regular bottom-up reporting of the issues • relevant for big organisations with complex structures	• focused only on these parts of the organisation which are involved in particularly risky activities/projects; • can be organised on more frequent basis than annual exercise	• small organisation/DG • non-homogenous activities of the Units • very specialised activities of the Units • annual or less frequent exercise - not performed regularly (time investment needed)

- *A balanced approach*: the approach and degree of top-management steer may vary from one DG to another and may **change over time**. Historically around 50% of DGs perform a high-level review or build the exercise around "risk themes" (risks pre-defined by top-management). Around 50% emphasise the bottom-up perspective (Units inform top-management about their most significant risks).

3.1.6. Stating activities and related objectives

- *The Management Plan (MP):* In line with the definition in section 1.1, risks relate to the non-achievement of objectives: the link between *Risk Management* and *planning and programming* is the MP. In the MP the DG's activities and objectives for the coming year are defined. Depending on the **scope and level of detail** of the Risk Management exercise, **different elements of the MP** can be used as a basis for the risk identification.

The Management Plan is built around the following concepts:

LEVEL OF DETAIL

- **General objectives** - The "general objectives" part contains a brief description of the mid or long-term vision for the policy area concerned and translates these into specific priorities for the reference year. It sets the framework for the activities of the DG. Typically there are 4 to 8 general objectives.
- **ABB activities:** ABB activities (Activity Based Budgeting) are defined in the ABB classification. For each ABB activity, the management plan indicates the title, a description and a justification for including it in the MP.
- **Specific objectives:** Specific objectives are the desired effects of the ABB activities. They are not a description of the activity itself but rather of its effect. For each ABB activity, at least one **specific objective** has to be defined. Typically, there are 5 to 10 specific objectives per Directorate.
- **Indicators**: For each ABB activity, at least one **result indicator** should be defined per specific objective. An indicator is information that should facilitate the monitoring of the objective's progress. **Result indicators** may be defined in terms of what should be delivered and at what time.

- *Activities or objectives?:* According to Risk Management principles, "objectives" (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, and as indicators aim at measuring progress towards achieving the objectives, any of the MP-elements (activities/objectives/indicators) can be used as considered appropriate by management;
- *Consider the style of the MP:* the way in which the MP is structured and written differs significantly between DGs. For example, for certain DGs, it makes sense to use result indicators to identify risks, whereas, for other DGs, these indicators may be too detailed for effective risk identification;
- *Define activities and related objectives clearly:* in any case, the activities/objectives/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. In the past, certain DGs experienced difficulties when using the MP for the Risk Management exercise, mainly because the activities/objectives/indicators stated in this document were unclear or not used by management in practice. In such a case, they may have to be reformulated or regrouped before using them in a Risk Management exercise. Where possible, objectives should be established according to the SMART-criteria (Specific, Measurable, Approved, Realistic and Timed). "The practical Guide for setting objectives and indicators" of April 2010 reflects good practices in this regard;
- *Timing:* for different reasons, the establishment and formal approval of the MP activities and objectives may sometimes be delayed. In this case, the Risk Management exercise **can be based on draft activities/objectives** and adapted at a later stage if necessary.

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 management plan exercise;

Table 3 - 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 ICC. 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 generic Risk Management questionnaire is available in Annex 4.	**+** 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 ICC/Risk Management coordination team 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 coordination team 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.

NEW!

Combination of several methodologies: depending on the particular situation of the DG/service (dealing with sensitive issues, organisation of the DG, number of staff, homogeneity of tasks etc.) a combination of several methodologies might be used for risk assessment. The table below shows a selection of strategies a DG may adopt depending on the objective of the exercise. The table is not exhaustive and the DGs are invited to adapt their strategies and methodologies to their particular circumstances.

Objective for the risk assessment exercise	Methodologies for risk identification
Completeness of information + targeting most risky projects	Survey addressed to representative number of staff (AD, AST, operational, horizontal etc.) + interviews with project management team
Awareness raising (involvement of staff) + assessing the quality of services	Workshops + survey addressed to stakeholders
Efficiency of the exercise + getting information about the sensitive issues	Desk review + targeted anonymous survey to staff

NEW! RISK TYPOLOGY BECOMES MANDATORY!

- *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 1) is there to ensure that the most common risk aspects are covered and that the risk categories used are consistent across all the Services. 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. Therefore the Commission's risk typology as presented in Annex 1 is **mandatory** for all Commission DGs and Services, **starting from the preparation of the MP 2011**;
- *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)? Good and less-good examples are provided in Table 4 below.

Table 4 - Examples of risk formulation:

ACTIVITY/OBJECTIVE: "To implement a new IT system for monitoring results of ex-post controls before the end of 2009"	
Risk formulation	**Comments**
"Failure to implement a new IT system for monitoring results of ex-post controls before the end of 2009."	**NOT OK:** This is simply the opposite of the objective.
"Lack of staff."	**NOT OK:** This does not give any information about the potential impact on the concerned activity/objective or about the precise cause of the risk.
"Lack of competent staff can lead to delays in the implementation."	**BETTER:** The impact on the objective is mentioned, although it is not very precise. However, there is no information on the cause of the risk.
"There is a risk of significant delay in the implementation of the project (rough estimation 10-12 months) because competent staff is not available. This is partly due to insufficient staff training."	**IDEAL**: There is a quantified estimation of the potential impact on the objective. The cause is also identified.

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.

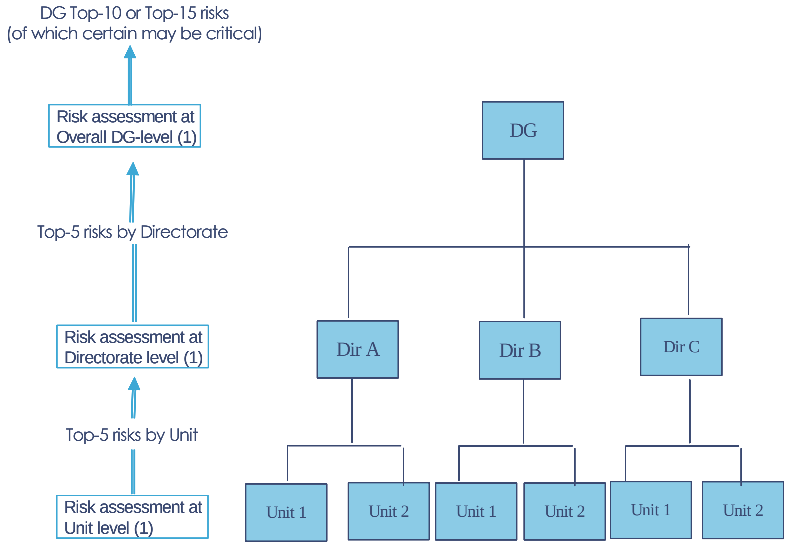
The list above is not exhaustive. It is to the responsibility of each Directorate-General to decide on the sources of information best adapted to their internal organisation and type of activity. Care should be taken before incorporating them into the risk assessment to ensure that external partners' views are relevant to the Commission'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;

- *Assessments at different levels:* in order to single out the most significant risks, assessments should be organised at different levels, as shown in the diagram below. 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. Note that the diagram below is just an example. **Depending on the scope** of the exercise, the assessment of risks can be organised differently.

Diagram 6 - Example of risk assessments ("bottom-up" approach):


DG Top-10 or Top-15 risks
(of which certain may be critical)
Risk assessment at Overall DG-level (1)
Top-5 risks by Directorate
Risk assessment at Directorate level (1)
Top-5 risks by Unit
Risk assessment at Unit level (1)
DG
Dir A
Dir B
Dir C
Unit 1
Unit 2
Unit 1
Unit 2
Unit 1
Unit 2

(1) It may not be feasible to assess all risks in the workshop. The ICC/Coordination Team can make a pre-selection of the risks to be discussed or regroup them by theme.

- *Preparing workshops:* in most cases, the risk assessment is performed via workshops/management meetings at different levels and prepared by the ICC. 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;

- *Keep it simple*: the impact/likelihood approach is used when assessing risks (see Annex 2). 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 5: Tips for conducting a workshop

Prior to the workshop
√ Designate the ICC 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 Director General - 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*: risks which meet the criteria set in SEC(2005)1327 are considered "critical". These critical risks must be reported in the DGs' Management Plan. It is always the **residual risk level** and not the inherent risk level that should be taken into account in defining criticality. For the definition of the residual and inherent risk please refer to the glossary;

- *Reporting format*: the reporting format is specified in the annual Standing Instructions for the Establishment of the MP issued by SG and DG Budget;

- *Overall DG perspective:* the identification of **critical risks** should be carried out from an overall-DG perspective. This is to ensure that the assessment is balanced and complete;

- *Formal validation of risks*: top-management validates the critical risks by reporting them in the MP. In addition, we recommend validating other significant risks via top-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 in the MP (and reporting in the AAR) so that no damage is caused to the Commission or its partners;

- *Link MP/AAR:* a critical risk reported in the Management Plan 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*

As mentioned in section 2.2.3 notification of potential critical cross-cutting risks to SG and DG BUDG is essential to the effective follow-up of those risks at the Commission level.

As of 2010, participation in the cross-cutting risk exercise became a formal obligation. The annual exercise is launched by a joint SG/ DG Budget note and DGs which do not face any cross-cutting risks should inform the Central Services accordingly by email.

All cross-cutting risks notified to SG/BUDG are recorded in a central cross-cutting risk register. All cross-cutting risks notified to SG/BUDG are subject to assessment. Based on the information provided, SG/BUDG determine whether notified risks are of a cross-cutting nature and whether they are potentially critical. It is important to highlight that the assessment by SG/BUDG is performed on the information provided by the DGs. No quality review of the adequacy of the mitigating actions is performed. As of 2009, in view of fostering greater transparency, Central Services do provide feedback on every cross-cutting risk which has been notified to them. A brief summary of this feedback is also registered in the cross-cutting risk register.

For cross-cutting risks which are potentially critical, peer-reviews are organised with the DGs concerned to assess the risk level, assign a chef de file and establish an action plan.

In order to detect additional cross-cutting risks not notified by the Services, SG/BUDG review all critical risks reported in the Management Plans and apply the same procedure (inclusion in risk register, assessment, organisation of a peer review,…) as for those critical risks which have been notified.

SG/BUDG, unless directly concerned, are not responsible for the implementation and monitoring of action plans. However, following each peer review SG/BUDG will invite the designated lead service(s) to ensure delivery of the actions decided upon. Accordingly, the designated lead service is responsible for ensuring delivery of the actions decided upon. DGs designated as lead service in the peer review will not systematically be invited to report on the actions taken and the residual risks.

Information about the status of peer reviews and the management of cross-cutting risks is should be included in the individual Annual Activity Reports. There is no central reporting on cross-cutting risks other than the cross-cutting risk register.

3.2.6. *Risk inter-dependencies*

Risks may be inter-dependent, meaning for example that if one risk becomes reality, this may have an impact on the DG's other activities. DGs should be alert to this possibility and take account of it in the risk assessment exercises.

a) Risk identification

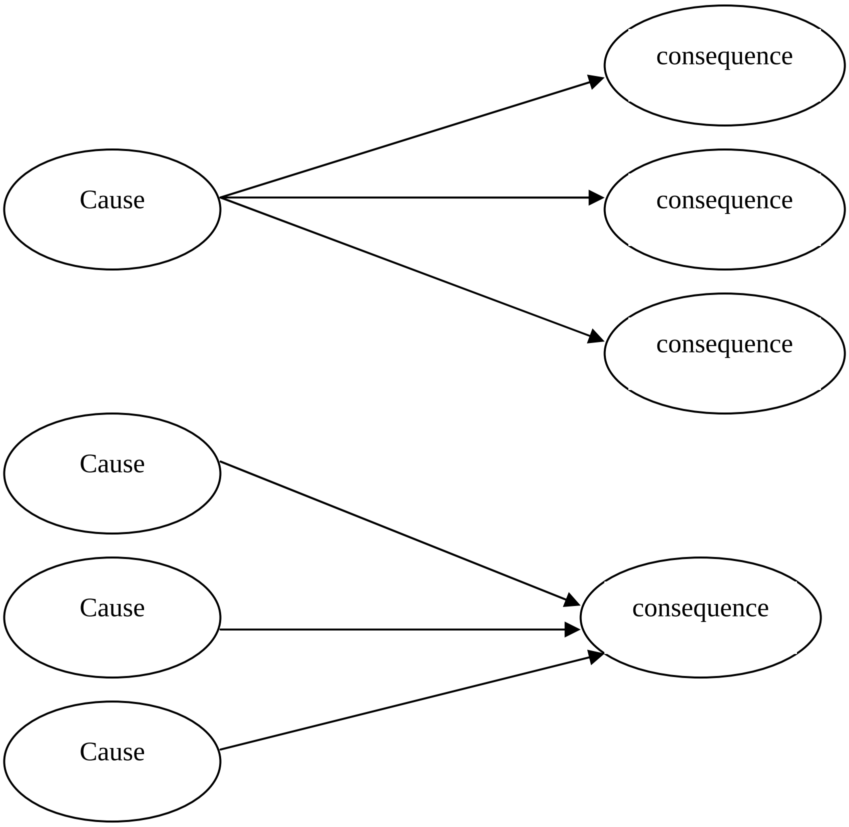
Cause → Consequence

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.

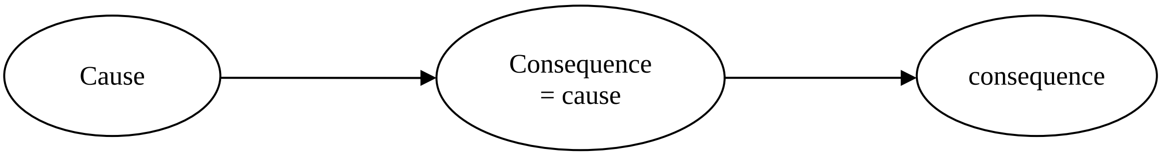
And the other way round: the risk may materialise only if several events which were defined as a cause happen at the same time.

Both situations are illustrated by diagram 7.

Diagram 7 - 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 DG (or even if relevant of other DGs):

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 DG'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 DG).

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

NEW!

3.3.1. Special case - risks outside management's control

Risks outside management's control fall into two categories:

- **risks outside the DG's control** - but within the control of other DGs and Commission services either alone or acting together. These are called "cross-cutting risks" and are the subject of separate guidance from the central services (http://www.cc.cec/budg/man/icrm/_doc/services/guidelines/doc_100922_crr_procedure_en.pdf);

- **risks outside the control of the Commission** - these risks fall mostly under category 1 ("Risks related to the external environment") of the Commission's Risk Typology (Annex 1). In the case of most of these risks the only possible answer is usually "*Accept*", though some measures to mitigate impact may be possible. As a result of the lack of direct control over this type of risk, we recommend that they are 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 and/or deficient institutional capacities in beneficiary countries having as a result that the Commission's political objectives are not possible to meet (e.g. humanitarian aid);
- failure of the engagement of Member States, authorities and stakeholders in the achievement of shared objectives;
- the risk of delays in implementation of the one of the crucial IT systems of the Commission 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 DG risk registers*: documenting the DG's **most significant risks** in a central risk register is **mandatory**. Typically the risk register should include all the significant risks identified in the DG (including the "critical risks");
- *Unit/Directorate risk registers*: in addition, it may also be useful to document each Unit's or Directorate's most significant risks in separate risk registers.
    - ➢ *Risk register format (Annex 3)*: the risk register should contain **as a minimum** the following information:
        - o risk description using the "cause - consequence" model. The risk level recorded should be assessed at its **residual** level (after controls existing in the organisation);
        - o risk type as per risk typology;
        - o Policy area/activity/objective affected by the risk;
        - o Proposed risk response;
        - o Action Plan (actions, owner, deadline).

Optionally the DGs might also include other information, such as: inherent risk level, controls in place, etc.

A proposed template risk register with all the **minimum mandatory information** is presented in Annex 3. DGs are invited, where considered necessary, to adapt this template to their specific needs and operations: in such cases the minimum mandatory content must be respected.

- *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 ICC.

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. We recommend including: risk description, action plan goals, target dates and milestones, action owners, specific actions to be taken, resources needed and monitoring/reporting arrangements.

Table 7- Example of an action plan

Risk Description	Risk of unauthorised access and leakage of confidential information due to insufficient IT system protection.
Action Plan Goals	A. Develop and implement new policy for IT protection B. Ensure that existing controls work as intended in practice.
Target Date Completion	A. March 2008 B. June. 2007
Owner	A. Director X / Unit Head C B. Director Y / Unit Head B
Actions to be taken/Milestones	A - Hire external IT consultant to draft IT policy (sign contract June 2007) - Draft policy (January 2008) B. - Perform detailed IAC review of relevant controls (January-March 2007) - Draft audit report (April 2007)
Resources Needed	A. Estimated budget xx EUR B. No extra resources needed
Monitoring	A. Bi-weekly progress meetings B. Regular audit supervision + management review of audit reports

- *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 ICC;
- *Coverage*: the monitoring of action plans should not be limited to the critical risks, but should also cover other significant risks in the DG (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 lack of regular information;
- *Reporting*: the results and conclusions of the monitoring should be documented and reported to the relevant management level. The Commissioner should be kept informed of the evolution of critical risks as part of the regular dialogue with the DG.

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 DG must define a follow-up (contingency) plan offsetting out the actions to be undertaken if the risk materialises. The Commission-wide crisis management and contingency planning is governed by ICS10, the Framework for Business Continuity Management and additional guidance.

The accepted critical risks at the level of the Unit/Directorate/ Directorate-General 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 Commission should the risk materialise;
- other Units/Directorates/Directorates-General involved in a contingency plan should the risk materialise.

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

3.4. Specific risk reviews (not directly linked to the MP)

- *A continuous process:* in addition to identifying risks directly associated with the MP, we recommend carrying 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?);

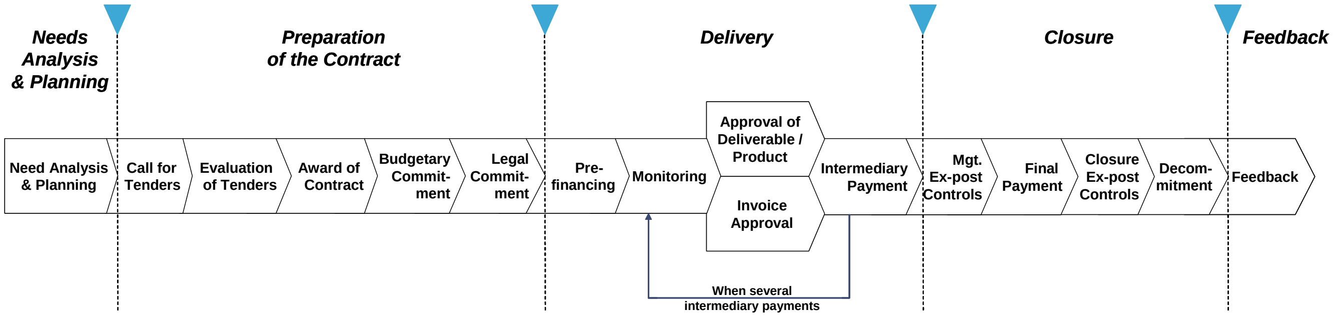
  (2) Identifying and assessing risks using the impact/likelihood method;

  (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 mangers are responsible for coordinating and carrying out specific risk reviews. They are assisted by relevant staff (and the ICC where appropriate) and if necessary by external specialists;
- *Scope and timing*: compared to an MP Risk Management exercise, 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 ICC should be informed of a specific risk review to keep the coherence of the DG risk management;
- *Flow-charting:* in order to prepare for the risk review, we recommend illustrating the concerned process/project/system graphically, 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.

***Diagram 8**: Flow-chart of the procurement process.*



- *Central guidance*: BUDG/CFS is developing guidance for specific risk reviews in certain areas. Currently, guidance for Risk Management related to procurement and IT Risk Management guidance is available. Other areas will be covered and published if necessary.

ANNEX 1 - RISK TYPOLOGY

NEW RISK TYPOLOGY BECOMES MANDATORY!

The Commission's risk typology (below) 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 Commission. 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).

Table 8 - Example of risks based on the risk typology

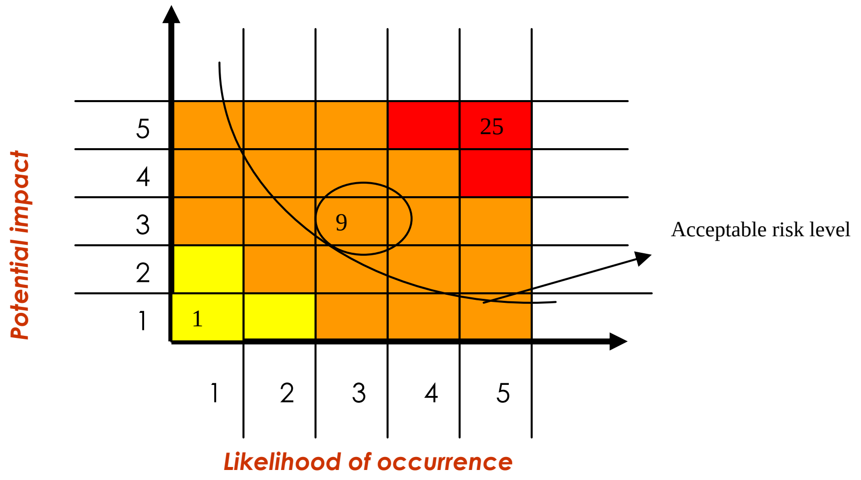
Main risk groups		**Examples of risks**
External	**1. Risks related to the external environment (outside DG/Commission)**	1.1 Examples of macro environmental risks: ▪ Humanitarian aid does not reach the dedicated population due to corruption/social instability/armed conflicts. ▪ Delays in the development of aid programs due to natural disasters, diseases, etc. 1.2 Examples of risks related to political decisions and priorities taken outside the Commission (European Parliament, Council, Member States, etc): ▪ Delays in the definition of the multi-annual work programme caused by the lack of agreement on the budget perspectives. ▪ Rejection by the Council of a Commission's legislative proposal caused by the non-involvement of stakeholders. ▪ Commission's objectives impacted by low political support in Member States. 1.3 Examples of risks related to external partners (Member States, EU institutions, National Agencies, Outsourcing, Consultants, media, etc.): ▪ Delays in the implementation of a specific programme due to poor performance by service provider/contractor. ▪ Delay in the payment of grants caused by inaccurate and late information transmitted by a Member State.
Internal	**2. Risks related to planning, processes and systems**	2.1 Examples of risks related to the strategy, planning and policy, including internal political decisions (APS, MP, etc.): ▪ Performance affected by unclear strategies or objectives. ▪ Expectation gaps caused by the absence of agreed performance targets. ▪ Contradictory objectives due to insufficient communication between DGs in planning phase. ▪ New demands and expectations by EU-citizens are not identified due to inappropriate/static planning process. 2.2 Examples of risks related to operational processes: ▪ Difficulties in implementing new policies caused by a lack of adequate legal instruments. ▪ Ineffective implementation of programs caused by cumbersome operational procedures. 2.3 Examples of risks related to financial processes and budget allocation: ▪ Loss of EU-funds caused by fraud. ▪ Payment of ineligible costs caused by unclear financial rules. ▪ Incoherence between objectives and available budget (unbalanced budget). 2.4 Examples of risks related to IT and other support systems: ▪ Operational performance affected by obsolete IT systems. ▪ Loss of critical data caused by the absence of a backup arrangements or insufficient virus protection. ▪ Leak of critical information caused by inappropriate IT profile or protection.

Main risk groups		Examples of risks
Internal	**3. Risks related to people and the organisation**	3.1 Examples of risks related to human resources (staffing, competences, collaboration): ▪ Excessive dependency on temporary staff or subcontractors. ▪ Reduction in available resources caused by unsatisfied staff leaving the service (e.g. due to an absence of feedback on their performance or of clear performance indicators). ▪ Implementation delays and errors caused by a lack of competence and expertise. 3.2 Examples of risks related to ethics and organisational behaviour ("tone at the top", fraud, conflict of interests, etc.): ▪ Adverse reputation and financial loss due to conflict of interests (e.g. discriminatory selection of contractors; usage of "insider information", etc.). ▪ Fraud or irregularities caused by a lax attitude towards rules and regulations. 3.3 Examples of risks related to the internal organisation: ▪ Operational performance affected by insufficient supervision arrangements. ▪ Delayed or ineffective decision making due to insufficient/inappropriate delegation of authorities. ▪ Frauds due to absence of segregation of duties. ▪ Inefficiencies due to absence of clear reporting lines. 3.4 Examples of risks related to the security of staff, buildings and equipment: ▪ Destruction of critical documents and damage to equipment caused by insufficient fire-protection. ▪ Theft of high-value equipment or sensitive information caused by insufficient access control to premises.
	4. Risks related to legality and regularity aspects	4.1 Examples of risks related to the clarity, adequacy and coherence of applicable laws, regulations and rules: ▪ Inequity in the evaluation of experts caused by interpretation of complex evaluation rules. ▪ Non-respect of procedure for selection of offers caused by complexity of the Commission's rule base. ▪ Acceptance of non-eligible claims caused by unclear rules and regulations. ▪ Impossibility of assessing the readiness of Candidate countries due to the complexity of the transposition rules of the "acquis".
	5. Risks related to communication and information	5.1 Examples of risks related to the communication methods and channels: ▪ Reputation of the Commission affected by insufficient communication to EU-citizens. ▪ Claims against the Commission due to disclosure of sensitive/confidential information. ▪ Operational performance affected by insufficient communication within or between DGs. 5.2 Examples of risks related to the quality and timeliness of information: ▪ Implementation of policies affected by non-reliability of available information, or delays in receiving the necessary data.

ANNEX 2 - RISK ASSESSMENT

Qualitative/Subjective Risk Assessments

***Diagram 9**: Risk assessment*



Most risks in the Commission are assessed using more or less **subjective judgements** of the impact and likelihood. A way of "measuring" the significance of such risks is to ask the persons participating in the assessment to indicate how they, on a given scale (1-5 - lowest to highest), would rate the likelihood and impact. The risk level is then calculated by combining the impact/likelihood, for example through applying the following equation:

Risk Level = Likelihood x Impact

For the sake of coherence between Services, the standard 1 to 5 scale **must be used**.

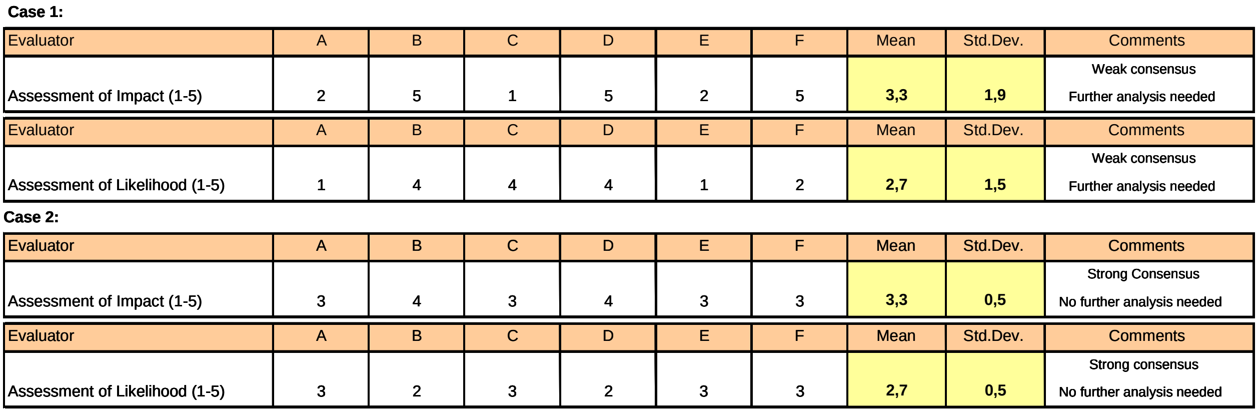
However, the "risk level" obtained through this approach can only be indicative and should therefore be **interpreted very carefully**. Since it is based on subjective judgements, it is generally not very meaningful to simply state that a risk of "16" is more significant than a risk of "15". The ratings should rather be used as a means of **detecting diverging opinions** among the assessors, which need to be further investigated. The numerical classification can however provide a rough ranking of the risks which may be further grouped into categories (for example High, Medium, Low).

If considered useful, the **consensus** among evaluators can be measured by calculating the standard deviation of the individual assessments. A small standard deviation (<1) indicates that the responses are clustered closely around the average value (mean) and that the consensus is high. A large standard deviation (>1) **indicates that there is little consensus** amongst evaluators. In that case, **more investigations**/analyses may be needed to evaluate the risk and examine the reasons for differences in perception.

It needs to be stressed that the methodology can be subject to manipulation or to particular sensitivity to risks (or lack of it) during the assessment process. As a result, the larger the group of evaluators, the more meaningful and representative the results will be. In smaller groups, in the case of major differences of opinion, consensus might be reached through constructive discussion.

Example: Measuring the consensus:

In Case 1 below, there is a weak consensus amongst the evaluators, both as regards the impact and likelihood (standard deviation 1.9 and 1.5 respectively). This suggests that more analyses and explanations about the potential impact and likelihood are needed. In Case 2, there is a very strong consensus:



Case 1:

Evaluator	A	B	C	D	E	F	Mean	Std.Dev.	Comments
Assessment of Impact (1-5)	2	5	1	5	2	5	3,3	1,9	Weak consensus Further analysis needed

Evaluator	A	B	C	D	E	F	Mean	Std.Dev.	Comments
Assessment of Likelihood (1-5)	1	4	4	4	1	2	2,7	1,5	Weak consensus Further analysis needed

Case 2:

Evaluator	A	B	C	D	E	F	Mean	Std.Dev.	Comments
Assessment of Impact (1-5)	3	4	3	4	3	3	3,3	0,5	Strong Consensus No further analysis needed

Evaluator	A	B	C	D	E	F	Mean	Std.Dev.	Comments
Assessment of Likelihood (1-5)	3	2	3	2	3	3	2,7	0,5	Strong consensus No further analysis needed

Quantitative/Objective Risk Assessments

A pure quantitative and thus **more objective** assessment of a risk is possible only where the DG can produce relevant and reliable data that can be used for **statistically valid projections/forecasts**. This is likely to be possible only in purely financial analysis - for example, if the error rate for a certain type of transaction has been very stable over the years, and provided that the control environment and systems have not changed significantly, it is probable that the error rate will remain at the same level in the future. The historical error rate, possibly adjusted, can thus be used as a basis for risk calculations.

ANNEX 3 - RISK REGISTER

NEW! RISK REGISTER BECOMES MANDATORY!

Risk title & Description (including cause and potential consequence)	**Risk type** (refer to risk typology)	**Policy area & Activity/ Objective affected**	**Residual Risk level ***	**Risk Response ****	**Action Plan Summary**		
					Brief description	Owner	Deadline
			- Critical risk (reported in AMP) - Other significant risk	Avoid/Transfer/ Reduce/Accept			

** risk are assessed always at their residual level (i.e. after taking into account controls existing in the organisation). The combined result of impact and likelihood of the residual risk using the common scale (1 to 5) should be inserted to the table.*

*** one of the 4 risk responses should be inserted to the table as a minimum information (for their own purposes DGs may add additional information).*

ANNEX 4 - GENERIC QUESTIONNAIRE FOR RISK IDENTIFICATION AND ASSESSMENT

This **generic** questionnaire is based on the Commission's **common risk typology**. The main purpose of the questionnaire is to help management and staff take into account all main risk aspects and domains when identifying the risks. It can also facilitate the consolidation of the identified risks at a central DG-level. It should be noted that certain risks may fit into several of the proposed risk groups. In that case, any of the concerned risk groups can be used.

The questionnaire is also available (just as the *ICAT questionnaire*) in ICMT (on request to BUDG ICMT SUPPORT mailbox). The ICMT-version facilitates the sorting and consolidating of risks and is therefore suitable when the number of survey participants is high. The Word-version can be used for smaller surveys and for structured interviews and workshops. To make it more effective, it can be **customised to the DG's specific needs**.

DG/Directorate/Unit	
Name	
Date	
List your entity's objectives/activities to be used as a basis for the risk identification	• • • • • • •

1. RISKS RELATED TO THE EXTERNAL ENVIRONMENT

1.1. **Macro-environment**: Can you identify any problems or potential issues related to the geo-political, macro-economic or social context in which the DG works that could affect any of your activities/objectives listed above? (Examples: political instability, social unrest, financial crisis, etc.). Also, are there any risks related to the natural environment that could impact your activities/objectives (natural disasters, diseases, etc.)?

Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

1.2 **Political decisions and priorities outside the Commission**: Does any of your activities/objectives directly depend on political decisions and priorities outside the Commission (e.g. Council, Parliament, Member State, etc.)? Can you identify any problems or potential issues that could affect the achievement of your objectives with regard to this? (Examples: lack of budget agreement, rejection of legislative proposals, etc.)

Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

1.3 **External partners**: Do you depend on any external partners for the implementation of your activities/goals (e.g. organisations, agencies, external contractors, etc.)? Are there any problems or potential issues as regards the cooperation with the external partners or the services provided? In what way could this affect your activities/objectives? (Examples: service delays, low service quality, unclear service agreements/service instructions, too much dependence on one single service provider, confidentiality-issues, etc.)

Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

2. RISKS RELATED TO PLANNING, PROCESSES AND SYSTEMS

2.1 **Strategy, Planning and Policy**: Can you identify any problems or potential issues as regards the strategy and annual planning that could affect your activities and the achievement of your objectives? (Examples: unclear strategy and objectives, insufficient planning and preparation, strategy and objectives not known by management/staff or insufficiently "anchored" in the organisation, expectations gaps among stakeholders, incoherence between long term strategy/annual objectives, etc.)

Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

2.2. **Operational processes**: What are the most important operational processes and procedures your entity depends on? Are there any problems or potential issues related to these that could affect your activities/objectives? (Examples: process "bottlenecks", cumbersome/unclear processes and procedures, etc.)

Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

2.3. **Financial processes and budget allocation**: Can you identify any problems or potential issues as regards the financial procedures and budget allocation that could affect the achievement of your objectives? (Examples: budget not well balanced compared to the objectives, unreliable or incomplete financial information affecting the budgetary process, etc.).

Risk #	Risk description (including cause of risk and potential consequence)	Impact	Likelihood	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

		(1 to 5)	(1 to 5)	

2.4. **IT and other support systems**: What are the most important IT-systems on which your entity depends? Are there any problems or potential issues related to these that could affect your activities/objectives? (Example: obsolete or cumbersome systems, data and system security issues, frequent system interruptions, data protection issues, etc.)

Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

3. RISKS RELATED TO THE PEOPLE AND ORGANISATION				
3.1. **Human resources**: Are there any specific problems or potential issues regarding the human resources in your entity that could affect your activities/objectives (Examples: lack of staff, competencies and expertise, too much dependence on temporary staff/contractors, high staff turnover, etc.)				
Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)
3.2. **Ethics and organisational behaviour**: Can you identify any problems or potential issues regarding the ethics and organisational behaviour in your DG/Directorate/Unit that could affect your entity and, indirectly, your activities/objectives? (Examples: conflict of interests, discriminatory treatment, unethical behaviour, management not leading by example, etc.).				
Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)
3.3. **Internal organisation**: Can you identify any problems or potential issues regarding the internal organisation of the DG/Directorate/Unit that could affect your activities/objectives? (Examples: unclear reporting lines and sharing of responsibilities, inadequate governance structure and supervisory arrangements, inadequate delegation of powers, etc.)				
Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

3.4. **Security of staff, buildings and equipment**: Can you identify any problems or potential issues related to the security of staff, buildings and equipment? (Examples: premise access control, physical working environment, fire protection, theft, security plans, etc.)				
Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

4. RISKS RELATED TO LEGALITY AND REGULARITY ASPECTS				
4.1 **Legality and regularity**: What are the most important rules and regulations related to your activities/objectives? Can you identify any specific problems or potential issues related to these that could impact the achievement of your objectives? (For example, the rules and legislation can be unclear/ambiguous, overly complex, obsolete, incoherent, not sufficiently known by the users, delayed/not available, etc.)				
Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)
4.2 **Other**: Are there any other problems or potential issues related to the compliance with applicable rules and regulations concerning your DG/Directorate/Unit?				
Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

5. RISKS RELATED TO COMMUNICATION AND INFORMATION

5.1. **Communication methods and channels**: Are the communication methods and channels concerning your DG/Directorate/Unit effective or are there any problems or potential issues within this domain that could affect your activities or the achievement of your objectives? (Examples: ineffective communication to/from external stakeholders about the Commission's objectives and performance, ineffective communication between DGs/EU-institutions, ineffective communication within the DG/Directorate/Unit)

Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

5.2. **Quality and timeliness of information**: What is the most important information you need to carry out your activities and achieve your objectives? Is that information generally reliable and available on time and or can you identify any problems or potential issues in this area? (For example, the information can be delayed, incomplete, biased, inaccurate, etc.)

Risk #	Risk description (including cause of risk and potential consequence)	Impact (1 to 5)	Likelihood (1 to 5)	Remarks (e.g. rationale for risk level, suggested actions, activity/objective affected, other relevant comments)

GLOSSARY

Critical risk: a risk should be considered critical if it can:

- jeopardize the realisation of major policy objectives;
- cause serious damage to the Commission's staff, partners or customers (Member States, companies, citizens, etc.);
- result in critical intervention at political level (Council, Parliament) regarding the Commission's performance;
- result in significant infringement of laws and regulations;
- result in material financial loss;
- in any way seriously impact the Commission'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.

Impact represents the effect on the objectives/activities in case the event or issue giving rise to the risk occur. Elaborate on its measurement - subjective however.

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

Likelihood represents the probability that, or the frequency with which, an event is expected to occur over a given time horizon. Elaborate on its measurement - subjective however, etc.

Most significant risks are significant risks which in view of Management are most likely to become critical in the future.

Objective represents what a DG/Directorate/Unit wants to achieve (e.g. political, strategic, 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 Commission'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 (other terms: **risk appetite**, **risk tolerance**)

Risk assessment is the overall process of risk analysis and risk evaluation; it is sometimes 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 Commission 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 DG's objectives/activities.

Strategic Planning and Programming (SPP) **cycle** is an annual cycle by which the Commission sets its political priorities, translates them into operational objectives and allocates its resources accordingly. Refer to the SPP/ABM guide:
http://www.cc.cec/home/dgserv/sg/i/spp/index.cfm?lang=en&page=what_spp

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 us via mail to BUDG MAILBOX D03 if you have any specific questions regarding Risk Management and Internal Control.
- *The ABM/SPP-guide*
- *COSO-ERM:* The principles of the Commissiosn's Risk Management methodology are based on the internationally recognised COSO-ERM framework