COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 20October 2005
SEC(2005)1327

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

COMMUNICATION TO THE COMMISSION FROM MS GRYBAUSKAITÉ IN ASSOCIATION WITH THE PRESIDENT AND VICE-PRESIDENT KALLAS

Towards an effective and coherent risk management in the Commission services

20 October 2005

TABLE OF CONTENTS

1. Why risk management matters 4
1.1. The context 4
1.2. Benefits of risk management 4
1.3. What has already been done? 5
1.4. Main challenges and critical success factors 6
2. Key principles and tools for managing risks in the Commission 6
2.1. A simple, realistic and focussed approach 6
2.2. Risk acceptance 7
2.3. A common language and risk typology 7
2.4. Focus on critical risks 8
2.5. Monitoring and reporting tools 8
3. Risk management implementation 9
3.1. The key actors, responsibilities and related risk management structures 9
3.2. The scope of risk management 10
3.2.1. When should structured risk management exercises be carried out? 10
3.2.2. Risk management as part of the strategy and planning process 10
4. Support for implementing risk management 11
4.1. Creating a supportive work environment 11
4.2. Improving risk management skills 11
4.3. Establishing effective communication 11
4.4. Guidance by central services 11
4.4.1. The Risk Management Implementation Guide 12
4.4.2. Generic guidance for risk identification 12
4.4.3. Specific guidance for certain activities 12
4.4.4. Expert advice 12
5. Implementation calendar 2005-2007 13
6. Conclusion 14

1. WHY RISK MANAGEMENT MATTERS

1.1. The context

The risk management of the internal control and management processes is not new in the Commission. However, after several years of implementation by the services, the need for a more coherent methodology and central support is recognised. Also, a more efficient reporting to the top management and political level in the institution is desirable in order to improve the decision making process.

In its 2004 Synthesis report[1], the Commission committed itself to set up a Commission-wide risk management approach. Such a methodology should embed risk management into the existing planning and decision making processes and develop the concept of accepting risks. It should also include in the medium-term the management of risks at a "Family of services"-level (cross-cutting risks) and strengthen the risk management culture prevailing in the Commission.

Also, the Communication on a Roadmap to an Integrated Internal Control Framework[2] emphasises the need for a common risk management methodology, and the European Court of Auditors encourages the Commission to implement action plans in relation to the management of risks[3].

The approach retained is results-oriented, proportionate and flexible. While keeping the ambition of implementing effectively a more coherent methodology from 2006 onwards, each service has to define how to organise itself internally and how to use in an optimal way the existing management tools in order to cope with their specific risks environment.

While this communication focuses on the management of all risks related to the internal control systems and processes of the services, the legislative proposals and major initiatives or programmes having a budgetary impact are subject to a specific risk management process being impact assessments and ex-ante evaluation. Both processes are of course complementary.

1.2. Benefits of risk management

In recent years, risk management has become a generally recognised management concept adopted by a large number of organisations, both in the commercial and public service sector.

---

1 COM(2005)256 of 15 June 2005

2 COM(2005)252 of 15.6.2005: "*introducing a common methodology for risk assessment, in particular to give assurance on the management of the risk of error in the underlying transaction*"

3 2004/C 293/01 of 30 November 2005, paragraph 1.79

In essence, a structured and proactive management of risks can help an organisation become more dynamic and forward-looking and increase the chances of achieving its objectives. In particular, it will help to:

- **Make more reasoned decisions**. All decisions, whereas they concern the "business-as-usual" or new ideas and opportunities, always involve a degree of uncertainty. Risk management can help management to justify its decisions with reasoned judgments of both intended and unintended outcomes.

- **Improve efficiency**. By adopting a risk-based approach, organisations can make better judgments about how systems can be improved, where resources should be allocated, or how to achieve a better balance between the level of risk and the cost of controls.

- **Reinforce the reliability of management systems**. Risk management forms an essential part of the management and control environment of all organisations.

As far as the European Commission is concerned, risk management will also help to:

- Improve and complete the current Strategic Planning and Programming (SPP)/Activity-based Management (ABM) performance management system by ensuring that the key risks related to our activities are duly taken into account.

- Reinforce the integrated internal control framework, thereby contributing towards achieving a positive statement of assurance.

1.3. What has already been done?

Risk management, which is one of the key elements in an effective internal control framework, is not new in the Commission. Commission services regularly perform a risk assessment exercise on their management and control systems as required by Internal Control Standard 11[4]. In 2001, a common risk management approach was introduced via the Internal Control and Risk Self-Assessment (ICRSA), and several DGs have taken their own initiatives in this domain. The Annual Activity Reports and the declarations on reasonable assurance of authorising officers by delegation with their potential reservations and action plans complement the current internal risk management in the services.

There are, however, gaps in the present risk management approach as the Commission does not yet have a consistent Commission-wide risk management

---

[4] SEC(2000)2203 of 13 December 2000, updated by SEC(2001) 2037 of 20 December 2001, states, as standard 11, that "*each DG shall systematically analyse risks in relation to its main activities at least once a year, develop action plans to address them and assign staff responsible for implementing those plans*".

methodology for DGs' internal processes and activities or objectives. This is the subject of the present communication.

1.4. Main challenges and critical success factors

Based on a review of successful implementations of risk management in other public organisations[5] as well as the lessons learned from the pilot exercise run in several Commission services[6] in late 2004/early 2005, a number of critical success factors for this project can be identified and in particular:

- Top-level political and management commitment devoted to handling risks;
- Simplicity and robustness of risk management processes;
- A critical mass of skills and expertise in the organisation to manage risks effectively;
- Reliable information on which Services could base their judgments about risks;
- A working environment encouraging management and staff to inform the hierarchy of potential issues and risks.

2. KEY PRINCIPLES AND TOOLS FOR MANAGING RISKS IN THE COMMISSION

2.1. A simple, realistic and focussed approach

Basically, the risk management process includes the following steps[7]:

- Defining the basis for the risk management exercise (for example, the annual activities and related objectives);
- Identifying and assessing the associated risks and managing them in line with accepted risk levels (defining the risk response and implementing the action plan);
- Keeping top management/Commissioners informed of critical risks and monitoring the implementation of action plans.

DGs must use a risk management approach that is adapted to their specific situation and needs. The aim is to strengthen the existing management structures and planning and decision-making processes by embedding risk management into them as a standard element. Tools, methods and related support to the DGs

---

5 Such as the UK central government, the Canadian government and the Flemish regional administration in Belgium.

6 AGRI, BUDG, EAC, ECHO, EMPL, JLS, RTD, TAXUD and the Delegations.

7 Refer to Appendix 2, which sets out in further detail the risk management process and its key elements.

will be available in order to optimise efforts and exchange experiences, but no 'one size fits all' solutions will be imposed.

2.2. Risk acceptance

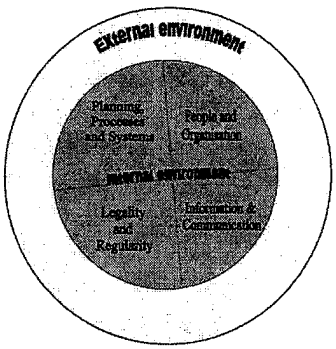
The purpose of risk management is not to avoid risks at all costs, but rather to ensure that the significant risks are identified and managed in line with accepted risk levels. Certain risks can be fully accepted, others not or only to a limited degree.

There are many reasons why certain risks have to be accepted. Firstly, reducing the risk to "zero" is usually not cost-effective. Secondly, taking risks is a necessary part of keeping an organisation dynamic and adapting it to a changing environment. Thirdly, certain risks are out of management's control and cannot be avoided without discontinuing the related activities.

Management must determine whether or not the key risks the service is exposed to can, or should, be accepted or if action must be taken to reduce them. In some cases, mainly as regards financial risks, this decision can be supported by quantitative estimations (potential financial impact, etc.) and pre-defined risk levels can then be established (e.g. tolerable error rates). In other cases, for example as regards reputational or political risks, the decision must be based on qualitative criteria and political and professional judgments.

2.3. A common language and risk typology

The common risk typology, used by both management and the 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 risk aspects and potential risk areas have been considered. And thirdly, the risk typology can be useful when analysing, consolidating and reporting risks.



The risk typology consists of five main risk areas:

(1) External environment. A good example of risk management in this domain is when potential issues and problems related to external stakeholders are anticipated by involving them in the planning process (for example civil society in the debate on sustainable development).

(2) Planning, processes and systems. An example in this domain is the 2002 overall assessment of the readiness of the Commission services to integrate the new Financial Regulation in their internal control systems.

(3) People and organisation. One example here is the way the Commission has to deal with the competition regulations, where the skills and

availability of adequate resources are essential for the effective handling of these issues.

(4) Legality and regularity. Non-compliance with inter-institutional procedures could lead to delayed decisions. Unclear or overly complex rules and regulations could negatively impact the effectiveness and efficiency of the operations.

(5) Communication and information. A potential risk in this domain could be, for example, the communication strategy for the Constitutional Treaty.

2.4. Focus on critical risks

In order to make risk management effective and keep the documentation and reporting down to a reasonable volume, it is important to single out and focus on critical risks.

In the Commission, a risk should be considered as *critical* if it can:

(1) endanger the realisation of major policy objectives;

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

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

(4) result in infringement of laws and regulations;

(5) result in material financial loss;

(6) put the safety of Commission's staff at stake;

(7) or in any way seriously impact the Commission's image and reputation.

2.5. Monitoring and reporting tools

Risks considered critical should be reported upon in the framework of the Activity Based Management cycle. DGs must however ensure that risks containing sensitive information are not disclosed in a way that may harm the Institution's decision making process, its partners or stakeholders. The precise format for reporting risks and corresponding action plans is defined in the relevant circulars.

The outcome of the risk management exercises must be documented in a structured fashion, hereafter called "risk register". The risk register is a service's internal document to which access is restricted[8]. Whereas the reporting of risks

---

[8] The "risk register" is an internal service document. Access to information therein is subject to Regulation (EC) n° 1049/2001 (in particular art.4) of the European Parliament and of the Council

in the AMP-document is annual, the risk register is a "living" document that is updated whenever there is a significant change in the DG's risk exposure, for example as a result of new or modified activities and objectives, re-organisations of management structures or systems or changes in the external working environment. In addition to the critical risks, the risk register can also cover other significant risks that require follow-up and it can be used to support the regular reporting to the Commissioner. An example of a risk register template (optional) will be provided in the Risk Management Implementation Guide.

The Annual Activity Report (AAR) must provide an overview of the critical risks encountered and their impact in relation to the achievement of objectives, including information about unforeseen risks that materialized or risks that could not be managed as planned.

3. RISK MANAGEMENT IMPLEMENTATION

3.1. The key actors, responsibilities and related risk management structures

As specified in the code of conduct for Commissioners[9], the Commissioner supervises the management of his/her Director-General or Head of Service and gives him/her, where necessary, guidelines or general instructions to put policies and priorities into practice. This requires that the Commissioner is aware of the critical risks related to the DG's activities, both from the political and the operational perspective. The consultation with the Commissioner regarding the Annual Management Plan[10] should therefore include a discussion about the DG's critical risks and the corresponding action plans. Information on critical risks should also be provided via the regular updates on internal control and audit. The reporting through the Annual Activity Reports will be used for increasing the Parliament's and the Council's awareness of risks and risk management in the Commission.

Each Director-General has the final responsibility of the management of his/ her service and will, in this context, customise the risk management strategy and approach to the DG's working environment and specific needs. This will include the definition of the corresponding roles and responsibilities. Each Director-General may appoint the Internal Control Coordinator (ICC) to be responsible for the coordination of risk management exercises in the DG, and actively supports the development of a strong risk management culture.

---

of 30 May 2001, regarding public access to EP, Council and Commission documents – OJ L 145 of 31/05/2001. Access will be granted to the European Court of Auditor as foreseen by the Treaty and, on request, to the European Parliament following the specific arrangements as foreseen in the framework agreement on relations between the European Parliament and the Commission (point 26 and annex 1).

9 SEC(2004) 1487/2 - Code of Conduct for Commissioners

10 SEC (2005) 1201

Finally, a comprehensive risk assessment has to take into account the entire "delivery chain", also involving the main external partners participating in the management of the Commission's activities (for example governmental organisations, agencies, outsourcing companies, etc.). The purpose is to obtain the external partners' view on potential risks that could impact the Commission's activities and objectives. Propositions as to how this can be organised in practice will be developed accordingly.

3.2. The scope of risk management

3.2.1. When should structured risk management exercises be carried out?

While risk management of "business-as-usual" is carried out continuously as a natural part of daily management (for example via regular management meetings, reviews, verifications, analyses, etc.), a more structured and documented risk management exercise needs to be carried out in case of significant changes in the DG's strategy, activities, systems and organisation, or in the external environment in which the services works.

In practical terms, structured and documented risk management exercises have to be carried out as part of the AMP process and, if the service considers it necessary, via complementary risk reviews of new or modified activities, when appropriate.

3.2.2. Risk management as part of the strategy and planning process

During the preparation of the AMP, each service will identify significant risks related to the foreseen activities and objectives. In order to ensure that all risk aspects are covered, the Commission's risk typology can be used to facilitate this exercise.

Although the scope of the risk management exercise has to be comprehensive, the focus will be on new or changed activities/objectives and modifications in the corresponding processes and systems, since change often represents the most significant risks.

Since the preparatory work for the AMP 2006 has already started in several DGs, the time schedule for 2005 is very tight and would therefore require a good coordination within the services and the identification of critical activities. The 2006 AMP exercise will be considered as an intermediate step towards the full implementation of the new concept, and expectations as to results have to be adjusted accordingly.

Once the integration of risk management within the AMP/AAR processes has been established, attention will have to be paid to the use of risk management to complement the basis on which assessment of priorities is carried out as regards resource allocations in the earlier phases of the Strategic Planning and Programming cycle, such as the Preliminary Draft Budget.

4. SUPPORT FOR IMPLEMENTING RISK MANAGEMENT

In order to ensure the successful implementation of risk management in a service and in the Commission as a whole, measures must be taken to ensure a supportive work environment, to build and improve risk management skills, and to establish effective communication.

4.1. Creating a supportive work environment

To make risk management effective, it is necessary to create and maintain a supportive work environment, i.e. to:

- ensure strong top management support;
- strive for a culture which does neither 'shoot the messenger' (reporting of risks must be considered positive) nor create excessive risks aversion;
- provide for the necessary instruments and tools;
- allocate sufficient time and resources for raising the awareness and develop risk management skills.

4.2. Improving risk management skills

The horizontal services, DG BUDG and DG ADMIN, will propose various training programmes for risk management: a general risk management training for managers and staff, a specific training for persons responsible for setting up risk management in a service (in particular the ICCs) and training to develop risk management facilitation skills (the organisation of management workshops, etc.). The DGs also have the option of developing customised risk management training programmes under an internal control framework contract with external consultants.

4.3. Establishing effective communication

Effective communication within and between the DGs is crucial. The ICC Network will be used to share best practices and experiences in risk management between DGs and services. A central risk management website will be developed by DG BUDG, and communication campaigns, presentations, and seminars will be organised in order to inform and raise awareness.

4.4. Guidance by central services

DG BUDG will support the implementation of risk management and facilitate the sharing of best practices between DGs. A risk management implementation guide and other relevant tools will be available and on-site facilitation will be provided. When executing its audits, the IAS will assess the efficiency and effectiveness of the risk management process.

4.4.1. *The Risk Management Implementation Guide*

A detailed guide providing practical advice and recommendations for how to implement and develop risk management in a service will be available. The guide will be regularly updated in the light of concrete experiences in the services.

4.4.2. *Generic guidance for risk identification*

An optional generic questionnaire based on the Commission's risk typology (see 2.3 and appendix 2) will facilitate the identification of risks. The purpose is to ensure that all risk aspects and risk domains are covered. The questionnaire will also facilitate the assessment and consolidation of the identified risks. To make it more effective, the DGs can customise the generic questionnaire to their working environment and specific activities.

4.4.3. *Specific guidance for certain activities*

As mentioned in 3.2.1, the DGs may decide to carry out additional risk management exercises of specific activities and initiatives during the year. In order to support the DGs, CFS will progressively develop central guidance in cooperation with the concerned horizontal services (SG, DG ADMIN and DIGIT). The guidance will focus on the following areas: 1) internal process leading to the adoption of legislative initiatives[11], 2) implementation of executive agencies, 3) procurement, 4) grants 5) development of IT-systems and 6) management of IT-structures in a DG. Ad-hoc advice will also be available.

4.4.4. *Expert advice*

The OGC Gateway Process[12] will be analysed in view of determining whether this methodology is appropriate for the Commission's environment. A pilot exercise will be organised in 2006 in order to validate the added value for the Commission services. The basic idea is that DGs could benefit from skills and experiences that exist in other Commission services as regards certain types of activities. It would thus be an effective way of sharing best practices between DGs.

---

[11] This guidance focussing on risks related to the internal process leading to the adoption of legislative initiatives is complementary to the Impact Assessments, which is a study designed to determine whether the outcome of the main proposed acts is sustainable and likely to improve the legislation currently in force.

[12] In simple terms, the OGC Gateway Process is a review of a delivery programme or procurement project carried out at a decision point by a team of experienced people independent of the project team. There are several reviews during the lifecycle of the project. The OGC Gateway Process is intended to provide assurance and support for the project owners so that the project can progress successfully.

5. IMPLEMENTATION CALENDAR 2005-2007[13]

The goals for 2005-2006 are to build and strengthen the risk management knowledge and processes at individual service level through the AMP process. DGs will start establishing bilateral contacts with partner DGs in order to identify cross-cutting risks and establish common action plans where this would be more effective for common activities. By 2007[14], the Commission will progressively address also how to deal with shared or cross-cutting risks in the most effective way, e.g. risks within "families of services" or risks related to similar management modes (e.g. DGs using executive agencies, networks of national agencies or contact points in Member States).

The key goals for **2005** are to:

- take a further step to increase awareness at senior management level of the need to integrate risk management in the planning and decision making processes by introducing it progressively in the 2006 AMP. Each Director-General should therefore define how risk management will be handled in his/her service and the allocation of individual responsibilities. Given the time constraints, the preparation of the 2006 AMP exercise will be considered as an intermediate step to introduce the new concepts. Expectations regarding the results should therefore be adjusted accordingly. The AMP circular provides more detailed information regarding the procedure to be followed;

- launch two training programmes: 1) specific training for staff responsible for setting up a risk management structure in a service (in particular the ICCs and their staff); and 2) workshops to develop risk management facilitation skills.

For **2006**, the main priorities will be:

- to strengthen and refine risk management within the AMP-process in order to progressively ensure the full coverage of all critical risks related to the DG's activities, objectives and processes;

- to provide progressively central guidance and advice for carrying out risk assessments in certain domains listed in 4.4.3;

- to underpin the communication strategy by setting up a central risk management website;

- to introduce in the first half of 2006, in addition to the two training programmes launched in 2005, a general risk management course for managers (in particular Heads of Unit), cabinets and key staff;

---

13 A global overview of the tasks to be carried out in 2005-2007 is given in Appendix 1.

14 2004 Synthesis Report, point 3.1.2.

– while gaining experience with risk management, including on issues common to several services, the directorates-general concerned start defining a common approach dealing with risks at "family of services" level and agree on concrete proposals;

In addition to further reinforcing risk management, the aim for **2007** is:

– based on the concrete proposals submitted and experience gained in 2006, to complement the methodology for dealing with risks at "family of services" level at the latest by March 2007 and implement it progressively in the AMP-process;

– to further develop a Commission-wide risk management methodology to be introduced at an earlier stage in the SPP cycle, for example via the Preliminary Draft Budget.

6. CONCLUSION

Risk management is not new in the Commission, but recent management and audit reports suggest that there is room for improvement, in particular as regards the development of a coherent Commission-wide approach; the integration of risk management into planning and decision-making processes; the use and development of "risk acceptance"; the monitoring of action plans; the management of risks at "family of services" level; and, not least, the development of a strong risk management culture.

The Commission is aware that the implementation of effective Commission-wide risk management is a long process that will require sustained support from top management, significant measures to build up the necessary risk management skills, and an approach that encourages the transparent reporting of risks.

Accordingly, the Commission is invited:

– to adopt the key principles and elements of the proposed risk management approach as presented in this document;

– to adopt the priorities for the 2005-2007 period as explained in the previous section;

– to confirm that the establishment and monitoring of the Annual Management Plan 2006 will constitute a further step in the identification, management and reporting of the critical risks as a step towards embedding the risk management process fully in regular management processes;

– to confirm the principles of a transparent reporting of risks as per section 2.4;

– to charge DG BUDG to include the considerations related to risk management in the annual Overview on the state of Internal Control in the Commission DGs and Services based on the information provided in the

DGs' Annual Activity Reports. On the other hand, as a simplification measure, the Mid-Term Update on Internal Control will only be maintained by DG Budget in case new elements or initiatives influence significantly the proposals of the annual overview.

- to invite each Commissioner to meet before the end of 2005 with his/her Director Generals to discuss, as part of the AMP process, the critical risks identified in relation to the activities and objectives foreseen for 2006[15];

- to instruct each Director General to review, based on the AMP 2006 experience, the risk management process for his/her service, including the definition of the corresponding roles and responsibilities inside the DG;

- to instruct each Director General to ensure appropriate training is followed and communication is carried out for strengthening awareness and developing the appropriate skills across all services;

- to charge the central services with developing the necessary guidance and providing the necessary assistance to the services for implementing this risk management approach in an effective way.

Therefore, each Commissioner is invited to actively follow up with his/her Directors-General the development of this risk management culture and its dissemination at all levels in the DGs.

---

15 Where the Director-General changes from January 2006, the hand-over process will include the risk management information.

Appendix 1: Global overview of the tasks to be carried out in 2005-2007

	2005	2006	2007
Main objectives	**At service level, progressive introduction of risk management in the AMP process, definition of the risk management approach and structures within the DG**	**Strengthening and refinement of risk management within the AMP process in order to progressively ensure the full coverage of all critical risks linked to the DG's activities, objectives and processes** **The directorates-general concerned start defining a common approach dealing with risks at "family of services" level and agree on concrete proposals**	**Complement the methodology for dealing with risks at "family of services" level at the latest by March 2007 and implement it progressively in the AMP-process** **Involvement of main external partners**
Introducing risk management in the AMP/SPP processes	Progressive introduction of risk management in the AMP process Possibility to focus on selected activities or objectives and limit the number of staff involved in the event of resource constraints	Strengthening and refinement of risk management at AMP level	Continuous reinforcement of risk management at AMP level Introducing risk management at an earlier stage in the SPP cycle
Risk Management Implementation Guide	First version of the guide (Oct. 2005), focusing on risk management related to the AMP process	Progressive update of the Guide based on the Services' practical experience.	
Optional Generic questionnaire for risk identification	Generic questionnaire (Oct. 2005) for the identification and assessment of risks	Enhancement of the questionnaire	

Central guidance in specific domains		Progressive development of central guidance for carrying out risk assessments in the areas cited in 4.4.3 (optional) Pilot exercise of the expert advice process	Continuation of central guidance in specific domains
DG BUDG support	Substantive advice and on-site facilitation when requested by the DGs, depending on available resources	Progressive development of adequate facilitation skills in the DGs, with BUDG providing substantive support and on-site facilitation again for this year	Less support, as DGs would then have "in-house" facilitation skills. DG Budget becomes more an advisor and communication hub for exchanging experiences
Training	- Launch of a specific training for persons responsible for setting up a risk management structure in a service (ICCs) - Workshops to develop risk management facilitation skills (for DG BUDG staff and ICCs)	- General risk management course for managers (Heads of Units) and key staff - 2005 training programs maintained	2005 and 2006 actions become permanent ADMIN training programmes
Communication	Various presentations on the risk management framework and its implementation at different management levels	Central risk management website and various information materials	Ongoing improvement of the website

Appendix 2 - Technical note on the Commission's risk management methodology

1. INTRODUCTION

This technical note provides some background information and a more detailed explanation of certain key concepts of the risk management methodology presented in the Communication *Towards an effective and coherent risk management in the Commission services*. Practical advice and guidance for the implementation of risk management in the Commission services will be provided in a separate document, the *Risk Management Implementation Guide*, of which a first draft will be available by October 2005.

The Commission's overall objective is to provide maximum value for its stakeholders — ultimately the EU citizens — in developing and implementing policies and programmes. In so doing, the Commission faces uncertainty, and the challenge for the institution and its management is to determine how much uncertainty to accept as it strives to deliver value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Risk management helps to effectively deal with uncertainty and associated risk and opportunity.

The Commission's risk management methodology as presented in the Communication is strongly inspired by the COSO Enterprise Risk Management Framework[16], which is considered best practice in this domain. It has however been adapted to fit the Commission's activities and specific working environment, notably through a pilot exercise carried out at the end of 2004 and at the beginning of 2005 involving 7 DGs as well as interviews with the remaining DGs. A visit in a Member State, which has a solid experience of implementing risk management in the public service sector, was also organised to identify best practices that could be relevant for the Commission. A Risk Management Steering Committee, including 3 horizontal services (BUDG, SG, IAS) and 6 operational DGs (AGRI, EAC, ELARG, EMPL, JLS and RTD), was created to determine the main principles and elements of the risk management framework, take strategic decisions, assure compliance with the needs of the operational services and keep the major players informed.

The implementation of an effective risk management requires strong political and top-management support and the development, or reinforcement, of a management culture in which the transparent communication of risks is encouraged and viewed as an instrument that can help management deal with risks in a more structured and proactive fashion.

It is also crucial that management and staff — as well as the Commission's stakeholders — fully understand the basic concept of risk management, i.e. that

---

[16] COSO (Committee of Sponsoring Organizations of the Treadway Commission) was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (known as the "Treadway Commission"). At the beginning of the nineties, COSO issued an Internal Control – Integrated Framework and in 2004 released the Enterprise Risk Management – Integrated Framework (COSO-ERM)

the aim is not to keep away from risks but rather to manage them in line with management's risk acceptance. Consequently, major efforts to inform and communicate will be necessary.

2. DEFINITIONS AND RISK TYPOLOGY

The Commission's definitions

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

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*".

These definitions reflect some fundamental concepts:

- *It is a process and a means to an end, not an end in itself*: risk management is not one event but a series of actions that are embedded in the Commission's activities, procedures and processes. These actions are inherent to the way the institution runs its activities and should be seen as part of a continuous cycle.

- *It involves people at every level of an organisation:* risk management is accomplished by the people in an organisation, by what they do and say at all levels of the organisation. This includes the Commissioners, management and staff. Everyone has responsibility at his/her level for risk management.

- *It provides "reasonable assurance"*: reasonable assurance reflects the notion of risk uncertainty. Risk management cannot guarantee that the objectives will be fully achieved. It can only provide "reasonable assurance".

- *It is based on "risk acceptance"*, which is the degree of risk that the Commission or a DG/Directorate/Unit is willing to accept in the pursuit of its goals[17].

The risk typology

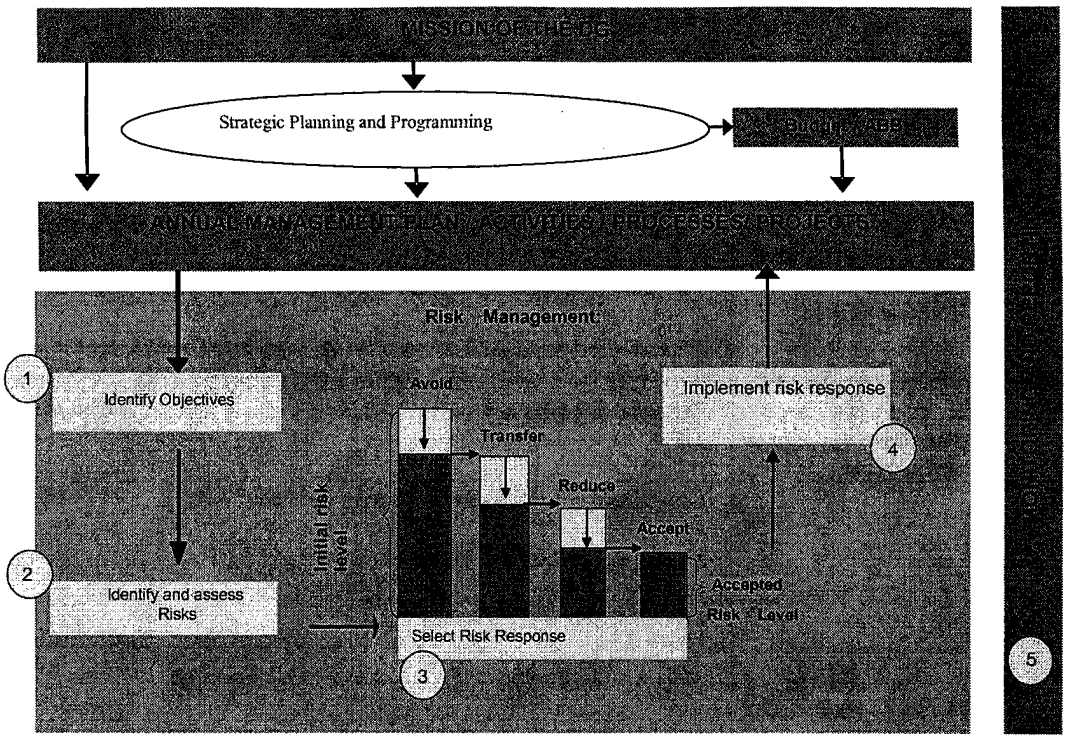
In order to facilitate the identification and reporting of risks, a common risk typology with 5 main risk groups has been defined:

[17] In international risk management frameworks, risk acceptance is also sometimes called "risk tolerance" or "risk appetite".

RISK TYPOLOGY		
Main risk groups		**Areas to consider when identifying potential issues and risks**
External	**1. Risks related to the external environment (outside DG/Commission)**	- Macro-environmental risks (geo-political, economic, natural disasters, etc.); - Political decisions and priorities outside the Commission (EP, Council, MS, etc.); - External partners (agencies, outsourcing, consultants, media, etc.)
Internal	**2. Risks related to planning, processes and systems**	- Strategy, planning and policy, including internal political decisions (APS, AMP, etc.) - Operational processes (process design and description) - Financial processes and budget allocation - IT and other support systems
	3. Risks related to people and the organisation	- Human resources (staffing, competences, collaboration) - Ethics and organisational behaviour ("tone at the top", fraud, conflict of interests, etc.) - Internal organisation (governance, roles and responsibilities, delegation, etc.) - Security of staff, buildings and equipment
	4. Risks related to legality and regularity aspects	- Clarity, adequacy and coherence of applicable laws, regulations and rules - Other potential issues related to legality and regularity
	5. Risks related to communication and information	- Communication methods and channels - Quality and timeliness of information

3. THE MAIN CONCEPT

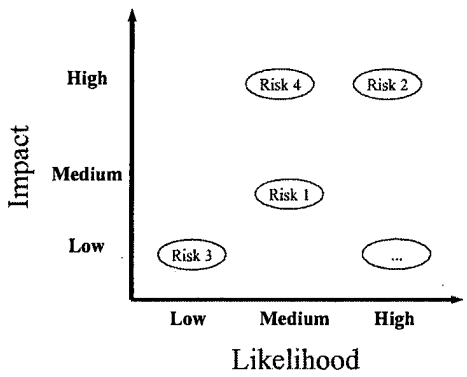
Risk management is not one single event but a series of actions that are embedded in the Commission's activities. These actions are integrated in the existing planning and decision-making processes and can be mapped in the following way:



(1) *Defining the basis for risk identification (objectives/activities)* — In principle, objectives must exist before management can identify potential risks affecting their achievement. However, as regards risk management related to the Annual Management Plan (AMP), the DGs can use either the annual activities or the related objectives as a basis for the identification of risks.

(2) *Identifying and assessing risks* — In this step, management identifies potential events and issues that, if they occur, will affect the achievement of the Commission's or DG's objectives (whether these objectives are political, strategic, operational or compliance-oriented). Risks are analysed and assessed in terms of their *likelihood* of occurrence and potential *impact* should they occur. This approach is illustrated in the figure below.

Example of impact / likelihood approach



Some examples of potential impacts are: policy objectives not realised, infringement of laws and regulations, financial loss, damage to the Commission's staff, partners or "customers" (Member States, companies, citizens) and adverse effect on reputation.

Once the potential impact has been defined and measured (for example low, medium, or high), management estimates the likelihood that the

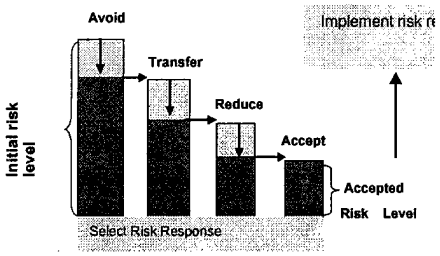
event leading to the impact will occur. In the next step, which is further explained in point 3 below, management will determine whether or not the risks can be accepted. In general, a risk with a low impact and a low likelihood of occurrence does not need any further consideration, whereas a risk with a high impact and high likelihood is unacceptable and will require priority action. However, this is a judgement that will depend on management's tolerance of risks, which may vary from one activity to another.

In some cases, it is possible to pre-define and quantify acceptable risk levels, e.g. in terms of financial impact. Management can for example decide beforehand that a financial loss higher than a fixed amount or a certain percentage of the budget for a specific programme is unacceptable.

As regards the risk level, it can be expressed either as the *inherent risk level* (the risk level in the absence of any existing controls and mitigating factors) or the *residual risk level* (the risk level taking into account existing controls and mitigating factors). To determine the residual risk level at the time of the risk assessment, the effectiveness and the efficiency of the existing controls must be considered. Thus, depending on the current residual risk level and management's risk tolerance, management will decide if additional measures are needed to further reduce the risk exposure. The time horizon used to assess risks should be consistent with the time horizon of the related strategy, activity and objectives.

(3) *Selecting the risk response* — There are in principle four possible ways of managing risks, or four "risk responses":

- *Avoid risk*: A risk can, for example, be partly or entirely avoided by modifying the activities or objectives. In certain cases, it may even be necessary to discontinue certain activities because the associated risks are considered unacceptable.



- *Transfer risk*: The risk is reduced by transferring or otherwise sharing a portion of it with a third party. A typical example of transferring risks is using an insurance company, which is paid to assume the risks. As far as *outsourcing* is concerned (i.e. when certain of the DG's activities or tasks are carried out by external companies), it should be noted that, although the management of the risk is transferred, the service remains ultimately responsible for the risks. However, it can be a good solution if the necessary resources, skills and competences to manage the risk are not available in the relevant service or even inside the Commission.

- *Reduce risk:* This is the most common risk response. Actions and decisions are taken to reduce the risk likelihood or impact, or both. This can be done in various ways, for example: enhancing the legislation, strengthening cooperation with partners, or increasing control efficiency and effectiveness by strengthening existing controls or implementing new ones, etc.

- *Accept risk:* Management estimates that the degree of risk exposure can, or has to be, accepted. Consequently, no further action to avoid, transfer or reduce the risk exposure needs be taken. Note that risks may have to be accepted for several reasons: firstly, reducing the risk exposure to "zero" would demand very significant control measures whose costs would be disproportionate to the benefits. Secondly, in order to adapt to a changing environment and new expectations, an organisation must continuously seize opportunities, modify its activities or try out new working methods, which may be risky. A static organisation adverse to change and innovation will soon become outdated and hence low-performing. Thirdly, certain risks are outside management's control. The only way of not being exposed to them would be to discontinue the activities concerned, which is not always possible or desirable.

(4) *Implementing the risk response (action plans).* Action plans are established and implemented to ensure that risk responses are effectively carried out. As a minimum, the action plan must include a description of the risk including the potential impact, the actions to be taken, the "owner" of the actions and the implementation target dates. Other relevant information such as resources needed for implementation and critical success factors may be added.

(5) *Monitoring and reporting*: In order to ensure that the action plans continue to be relevant and effective, management should carry out monitoring and supervision of their implementation on a regular basis. Since already identified risks may evolve and new risks may emerge, monitoring is also needed to ensure that the DG's risk register is up-to-date. Furthermore, top management and Commissioners must be kept informed of the evolution of critical risks, the level of risk acceptance and the emergence of new risks on an ongoing basis.