RISK MANAGEMENT GUIDELINES

FOR

COUNCIL OF EUROPE STAFF

Version 1.0 – 28 June 2016

TABLE OF CONTENTS

1. Managing risk at the Council of Europe 3
   1.1 Institutional framework 3
   1.2 Defining Risk and Risk Management 3
   1.3 Main Principles 4
   1.4 Risk Management Roles and Responsibilities 4
2. The Risk Management process – practical steps 7
   2.1 Identifying risks 7
      2.1.1 Selecting risks 7
      2.1.2 Formulating risks 8
      2.1.3 Categorising risks 9
   2.2 Assessing risk 9
   2.3 Addressing risks 10
      2.3.1 Accepting the risk 10
      2.3.2 Treating the risk 10
   2.4 Reporting on risks – Risk registers and escalation of risks 11
      2.4.1 Operational Risk registers 11
      2.4.2 Strategic/Organisational Risk Register 12
      2.4.3 Reporting to the Committee of Ministers 12

APPENDIX 1: Risk likelihood scoring 13

APPENDIX 2: Risk impact scoring 14

APPENDIX 3: Risk exposure 15

APPENDIX 4: Operational Risk Register – Template 16

1. MANAGING RISK AT THE COUNCIL OF EUROPE

Private or public, no organisation has the luxury of functioning in a risk-free context. The nature of the mandate and services of the Council of Europe is such that it has to operate at times in complex and unstable environments, which expose it to risks.

The Council of Europe's approach to risk management aims to facilitate managers' approach to risk and to increase the ability to identify and mitigate risks that may affect the achievement of objectives through a practical, structured and pragmatic approach to risk without overburdening management.

1.1 INSTITUTIONAL FRAMEWORK

The Financial Regulations require the Secretary General to "put in place a governance system, including notably: **risk management**, internal control, internal audit, performance indicators and evaluation of results".

In January 2014, a decision was taken in the Senior Management Group to introduce Council of Europe-wide Risk Management.

A first Strategic Risk Register was developed and adopted by the Senior Management Group in February 2016; on that occasion, the Secretary General concluded that the Council of Europe would continue with its work on risk management and that, in line with the recommendations of the External Auditor and the Oversight Advisory Committee, the overall responsibility for the co-ordination of risk management within the organisation would pass from DIO to the Directorate General of Administration (DGA) and the Office of the Directorate General of Programmes (ODGP).

On 28 June 2016 the Secretary General approved the Risk Management policy.

1.2 DEFINING RISK AND RISK MANAGEMENT

Risk Management implies to be proactive in recognising and managing **uncertain events that can have an effect on objectives**; it allows reducing negative consequences, seizing opportunities and ultimately improving an organisation's chances to reach its objectives within budget and timeline.

Term	Definition
Risk[1]	The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.
Risk Management[2]	A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organisation's objectives.

[1] Institute of Internal Auditors: International Professional Practices Framework.
[2] Ibid.

1.3 MAIN PRINCIPLES

Risk management is about being aware of risks and making decisions on how to deal with them. The Council of Europe's risk management reflects the following principles:

- Anticipate and manage risk: When developing strategies, action plans, work plans, designing or reviewing programmes, projects or activities, staff members should consider risks to the achievement of expected results;
- Avoid unnecessary risk: There is no benefit in accepting a risk if it does not help to advance towards objectives;
- Accept risk when benefits outweigh costs of eliminating/mitigating risk: Total risk elimination might not be possible or be excessively costly; value for money considerations must be taken into account;
- Make risk management decisions at the right level: Take decisions on risks at the level of delegated authority; do not assume risks for which authority has not been given to you; escalate the risk to a higher level of management when necessary;
- Do not take risk management as an exact science: It is based on professional judgment and constitutes a support to good managerial practices.

1.4 RISK MANAGEMENT ROLES AND RESPONSIBILITIES

The responsibility for operational risk management lies primarily with the Programme Coordinator[3] who is responsible for taking risk management decisions related to his/her Programme and is accountable for the content of the Programme **Operational Risk Register**.

Each Programme Coordinator should conduct a formal risk assessment at least once a year, or whenever a major change in the context occurs. It can be conducted as part of the annual Programme and Budget preparation/monitoring process and should ensure that key risks are identified, assessed and responded to (mitigating actions).

Risk Focal Points can be appointed by the Commitment Officers to co-ordinate risk management within their respective MAE and carry out the following tasks:

- Co-ordinating with Programme teams to ensure that Risk Registers are updated on time in accordance with the risk management policy and guidelines.
- Liaising with the Risk Working Group for completion/preparation of strategic risk registers and updating of risk management guidelines.
- Providing help and advice to programme coordinators filling out risk registers. Reviewing risk registers with Commitment Officers.
- Escalating issues to Commitment Officers as appropriate, e.g. regarding non respect of policy, follow up of mitigating actions and risks identified which require immediate action.

Risks should be escalated to more senior staff within the administrative entity or to Commitment Officers who can decide to escalate and submit them to the attention of the Risk Management Working Group that is in charge of preparing the **Strategic Risk Register**.

[3] The term Programme Coordinator refers to the person responsible for a Programme Line as included in the CoE Programme and Budget document.

The chart below illustrates the main Risk Management roles and responsibilities in the Council of Europe.

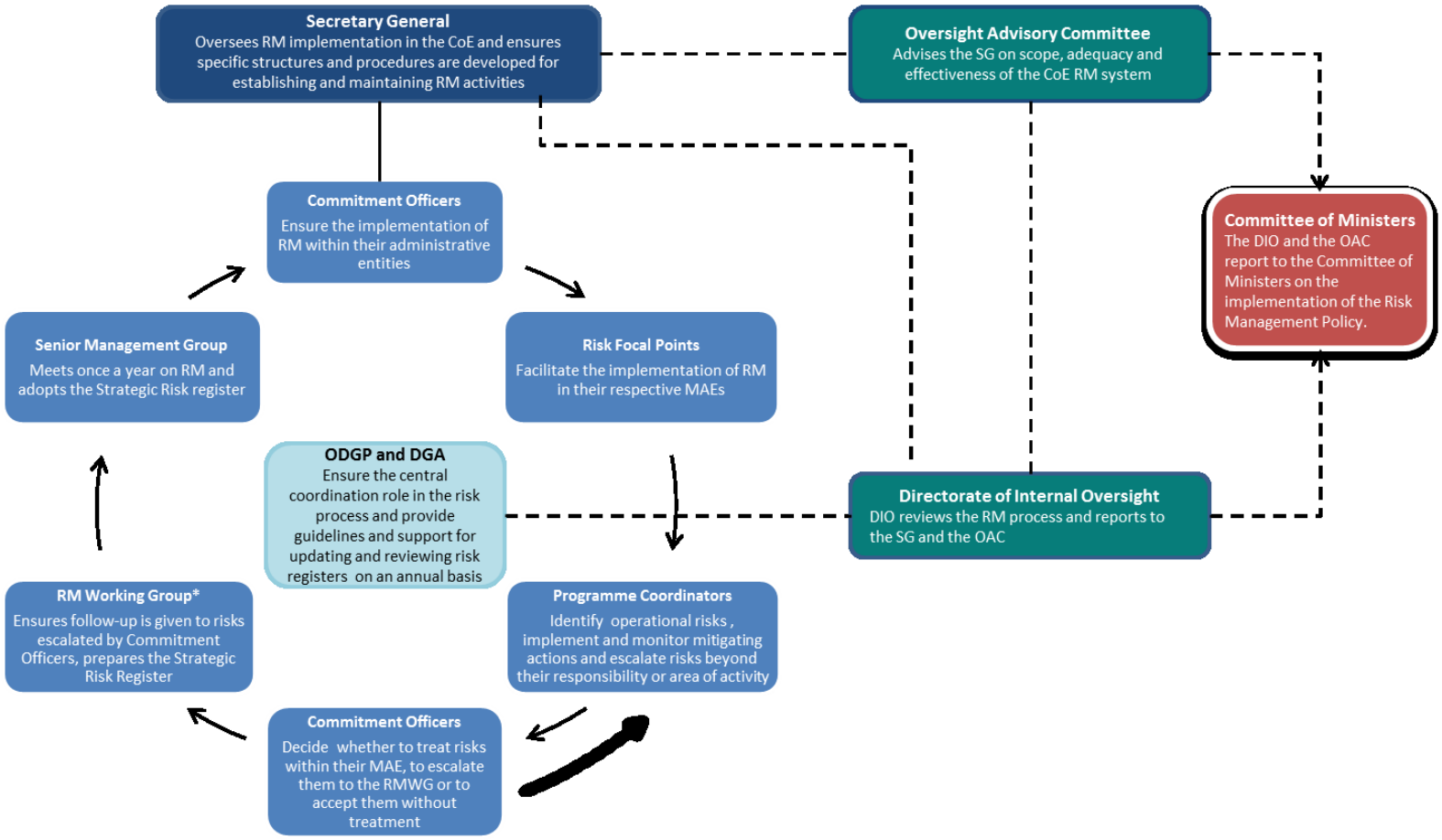
Risk registers should also indicate the following information:

- An identified **Risk Manager** who is responsible for identifying the risk, monitoring its evolution and implementing the mitigating actions. The Risk Manager is designated by the **Risk Owner** who is the senior manager that has the authority and accountability for risks within the Programme.
- Timeframes (dates for review and completion dates for mitigating actions to be implemented).

Basic risk management principles set out in these guidelines apply also to projects. The **Project Management Methodology** (PMM) Handbook gives brief information on project–level risk management. It is complemented with a risk template and other information that are available on the website www.coe.int/pmm.

The Council of Europe has also commissioned the preparation of a "**Document Unique d'Evaluation des Risques**" (DUER) which deals primarily with risks and mitigating actions related to health and safety at work. The DUER is prepared and updated in compliance with the *EU Directive n° 89/391/CEE on the introduction of measures to encourage improvements in the safety and health of workers at work* which was transposed in the French legislation through the *decree n°2001-1016*. As a consequence, the DUER is prepared and updated according to specific requirements but is part of the overall RM efforts of the Organisation.

Overview of the CoE organisational Risk Management Cycle
Roles and Responsibilities



*** RM working Group is chaired by a Staff Member appointed by the Secretary General; its members are the Risk Focal Points who represent Commitment Officers; its Secretariat is provided by ODGP and DGA.**

2. THE RISK MANAGEMENT PROCESS – PRACTICAL STEPS

The Risk Management process is usually organised in four main stages:

1. Identifying risks;
2. Assessing risks (their likelihood and potential impact);
3. Addressing risks (mitigating the occurrence or impact of adverse events);
4. Reviewing and reporting on risks.

2.1 IDENTIFYING RISKS

The starting point of programme operational risk identification is the relevant programme objective/expected results[4] as per the Programme and Budget document.[5]

2.1.1 Selecting risks

Risks that can jeopardise the achievement of objectives/expected results stem from external and internal causes.

- **External causes** relate to outside events or conditions. They may include threats such as a sudden onset of a political crisis or opportunities such as a change in government policy or new partnerships. Such risks may be beyond the organisation's immediate control, but must be recognised and managed.
- **Internal causes** may have to do with the adequacy of the organisational policies, capacities, organisational arrangements, resources, or other issues.

Several techniques can be used to identify risks; hereafter a non-exhaustive set that can be used individually or in combination in order to help identify uncertainties:

- Consult colleagues through brainstorming, workshops, etc. The best risk assessments always rely on a multitude of perspectives.
- Challenge and question assumptions: are they too optimistic/pessimistic? Is there any bias in the assumptions[6]?
- Identify key milestones and consider events that can throw you off course or those that are critical to help you achieve milestones and objectives.
- Ask “what if” questions, for example: what if a supplier goes bankrupt during a critical project? What if there is a sudden change in the political situation affecting the support given by the country to the project? What if the necessary expertise is not available within the timeframe imposed by the project?
- Consider the history of risks/incidents in your area of work and the plausibility that similar events may occur in the future.
- Consult evaluation and audit reports relevant to your unit and functional area.

[4] Expected results, can be used in order to clarify the scope of the Programme objective and to render it more concrete, therefore facilitating the identification of risks.

[5] Risks identified at the Programme Line level include risks for activities funded both by the Ordinary Budget and Extra-budgetary resources (Joint Programmes and Voluntary Contributions).

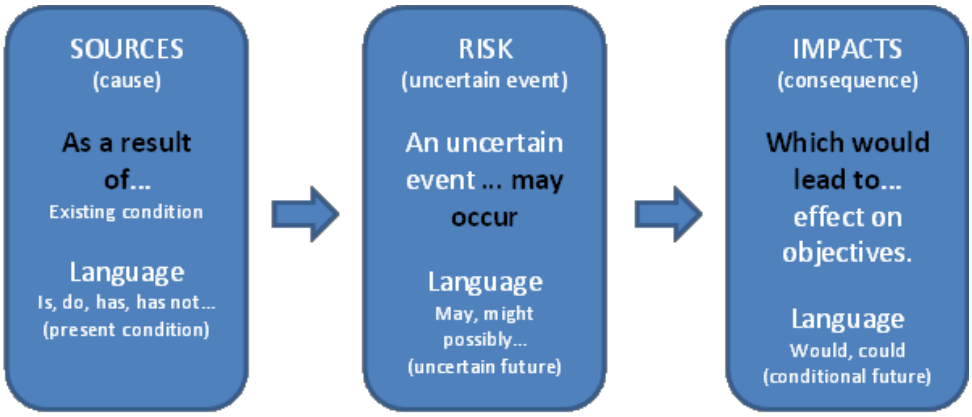
[6] Assumptions refer to any external factors that are relied on to be true for the realisation of a project’s expected results and objectives.

- Spend some time focusing on the exception rather than the norm. Think wider than given facts and brainstorm the not-so-obvious risks. Avoid re-using previous risk assessments and formulations.

2.1.2 Formulating risks

Once identified, a risk must be clearly stated. To avoid inadequate risk formulation, make sure that the risk description:

1. relates to the objective/expected result whose achievement is at risk;
2. states both the cause and effect
3. does not simply state the opposite of the objective.



Example of risk descriptions:

As a result of the current CoE recruitment policy and procedures, a delay in the hiring process may occur for key experts to be involved in the pre-electoral assistance activities which would lead to the impossibility of implementing the proposed actions in time for the subsequent elections.

As a result of the current political instability in the country, a change of Government may occur and the national authorities may not provide the anticipated necessary support to the programme which would lead to non-implementation of proposed changes in legislation.

As a result of insufficient investments in IT equipment (audio, video, voting system) in the CM room, IT incidents may occur and disrupt the work of the CoE decision-making body which would lead to delayed and/or ill-informed decision-making.

As a result of the current increase in terrorist attacks, incidents may occur to CoE officers on mission which could lead to suspending missions and/or programme implementation.

2.1.3 Categorising risks

Risks have to be associated to one of the following categories, on the basis of their nature.

Risk category	Definition	Examples
Safety, security and logistics	Risks related to the management of human and material resources and their security	As a result of CoE staff taking positions on sensitive matters and affecting political and economic interests, they might be personally and physically attacked, which could lead to…
Communication and reputation	Risks related to communication management and to the promotion of the organisation's image and reputation	Due to staff not being fully aware of the Organisation's communication protocols non-authorised statements might be issued in relation to projects which would lead to …
Political	Risks related to political decisions taken within the Organisation (Committee of Ministers, Parliamentary Assembly,…), in other stakeholder organisations and/or in Member States	Due to the current CoE criticism vis-à-vis [*Member state*] and the related sanctions decided by CoE bodies, [*Member State*] might decide to leave the organisation, which would lead to…
Project/Programme delivery	Risks related to project/programme delivery (planning, management, procurement, specific expertise,…)	Due to financial problems, the project partner selected through the appropriate tendering procedure might discontinue its activities and not be in the position of delivering the agreed upon services, which would lead to…
Human resources	Risks related to HR management	Due to the current restrictions on the length/stability of contracts, candidates having succeeded in competitive examinations might decide not to accept employment proposals, which would lead to…
Financial	Risks related to finance, accounting, treasury, processes	Due to fluctuating currency rates, the voluntary contributions provided in currencies other than euros might result in amounts in euros lower than foreseen, which would lead to…
IT	Risks related to management and security of information systems	Due to hacker intrusion IT system breakdowns might occur increasingly frequently, which would lead to…

2.2 ASSESSING RISK

Risks should be assessed taking into account all mitigation measures that are already in place[7].

A risk may have a major impact when it occurs, but the likelihood of it happening may be very remote. Conversely, a risk with a rather minor impact may turn into a major risk if it occurs repeatedly. These two parameters are synthesised with the concept of "exposure".

Exposure is defined as the combined effect of the Impact of the risk, should the event occur, **and the Likelihood** of occurrence **(Exposure = Likelihood multiplied by Impact)**.

Likelihood is scored considering frequency or probability, on a scale from 1 to 4.

[7] This concept is known as residual risk

Impact is assessed based on a thorough judgement of the possible impact of the risk in question materialising, keeping in mind the following five types of impact: Programme delivery, Reputation, Financial loss, Human resources, Ability to operate. Impact is scored on a scale from 1 to 4.

Exposures are displayed as indicated in Appendix 3.

Except in the relatively rare case where statistical data are available, **the assessment process relies on informed but subjective judgment**. A CoE approach to likelihood and impact scoring is outlined in Appendices 1 and 2, respectively.

2.3 ADDRESSING RISKS

Depending on the level of exposure and risk appetite[8], a decision must be taken whether to:

- accept the risk or
- treat the risk by:
  - i) Avoiding the risk,
  - ii) Transferring the risk or
  - iii) Controlling the risk.

2.3.1 Accepting the risk

A risk is called acceptable if it is not going to be treated. Accepting a risk does not imply that the risk is insignificant. Risks may be accepted for a number of reasons:

- The level of the risk is so low that based on, for example, a cost benefit analysis, specific treatment is not considered adequate;
- The risk is such that no treatment option is available. For example, the risk that a project might be terminated following a change of government is not within the control of the CoE;
- The opportunities presented outweigh the threats to such a degree that acceptance of the risk is justified although it may still be mitigated

2.3.2 Treating the risk

There are three basic methods of treating the risk, these are:

a) Avoiding the Risk
   This is achieved by either deciding not to proceed with the activity that contains an unacceptable risk, choosing an alternate more acceptable activity, which meets the objectives and goals of the organisation, or choosing an alternative and less risky methodology or process within the activity.
b) Transferring the Risk
   Risk transfer transmits the organisation's risk to an outside party. The most common method of risk transfer is the purchase of insurance.
c) Controlling the Risk

[8] Risk Appetite is defined as the amount and type of risk that the organisation is willing to accept in order to meet Objectives. The level of risk appetite depends on the nature and type of activities under consideration. For example the Risk Appetite in terms of Treasury management within DPFL will be different to that within a programme or project operating in post conflict areas.

Risk control focuses on mitigating the likelihood of the risk occurring or the impact of the risk if it occurs, or both.

The mitigation plans should include:

- Proposed actions
- The person responsible for implementing the identified actions
- Timeframes (dates for review and completion dates for each action to be implemented)

2.4 REPORTING ON RISKS – RISK REGISTERS AND ESCALATION OF RISKS

The basic risk management tools are risk registers. Two main types or risk register are foreseen at the Council of Europe: **Operational Risk Registers and a Strategic Risk Register** (or Organisational Risk Register).

In line with the CoE Project Management Methodology, cooperation projects and programmes should have their specific risk registers (see PMM Handbook 2016).

2.4.1 Operational Risk registers

An operational risk register should be prepared for each Programme, taking as a starting point the objectives/expected results of the Programme Lines contained in the CoE Programme and Budget document**.**

As a general principle, a Programme Coordinator is responsible for preparing the Operational Risk Register for the programme under his/her responsibility (see Appendix 4 for an Operational Risk Register template) and for addressing those risks.

There are four main exceptions to this general rule, for which the good practice is to "escalate" the risk:

- When the assessed risk exposure, after the Programme Co-ordinator has implemented all mitigating actions possible with available resources, exceeds the risk appetite[9] (i.e. even after all mitigating actions have been implemented the Programme Co-ordinator thinks that the exposure to the risk is still too high.)
- When the nature of the risk is such that the Programme Coordinator has no competence and/or authority in that particular field.
- When the possible mitigating actions go beyond the functional boundaries of the Programme Coordinator.
- When a risk is shared with other Programmes/Entities or other functions of the organisation, or it is shared with external organisations and coordination is needed to find appropriate mitigating actions that can suit all the stakeholders.

Programme Coordinators might also wish to escalate risks specific to projects implemented for or in a specific country that could have an important impact on the Organisation's objectives.

[9] It is the responsibility of the Programme Coordinator to decide whether the risk assessment should be escalated.

In these cases, the risk must be escalated to the relevant Commitment Officers via the Risk Focal Points and, if relevant, to the Risk Management Working Group so that a decision on the follow-up to be given can be taken. The Risk Management Working Group may decide to include the risk in the Strategic Risk Register or to allocate the risk to another Programme so that is can be appropriately managed. In the latter case, the risk and its mitigating actions will have to be introduced in the relevant risk register.

2.4.2 Strategic/Organisational Risk Register

The Strategic or Organisational Risk Register responds to the need of governing bodies and senior management to understand and to address the risks which might affect the organisation's strategic objectives.

The preparation process of the Strategic Risk Register relies on a bottom-up and a top-down approach:

- The bottom-up component relates to the risks which are escalated by Programme Coordinators (see previous paragraphs) and is aimed to ensure a comprehensive identification of all important exposures. It helps, for example, managers to spot a problematic policy or weak operational procedure and escalate it to the appropriate managerial level so that a decision can be taken.
- The top-down system's objectives are to distil and provide clarity on the most important risks affecting the organisation's performance, support risk-informed decisions at the top management level and ensure a risk dialogue at governance level. The top down system is performed by the Risk Management Working Group which reviews the overall risk profile of the organisation, discusses the risks surrounding major decisions and addresses "hot topics" surfaced by the organisation's bottom-up system.

The Strategic Risk register is prepared by the Risk Management Working Group. It is discussed and adopted by the Senior Management Group.

2.4.3 Reporting to the Committee of Ministers

Both the operational and strategic risk registers are internal management tools; reporting to the Committee of Ministers on the implementation of Risk Management is done through the OAC and DIO annual reports.

APPENDIX 1: RISK LIKELIHOOD SCORING

Likelihood scoring is based on the knowledge and actual experience of the individual/group assigning the score. In assessing likelihood, it is important to consider the nature of the risk. Risks are assessed on the probability of future occurrence; how likely is the risk to occur? How frequently has this occurred?

It should be noted that in assessing risk, the likelihood of a particular risk materialising depends upon the effectiveness of existing controls; consideration should be given to the number and robustness of existing controls in place, with evidence available to support this assessment.

The assessment of likelihood of a risk occurring is assigned a number from 1 (unlikely) to 4 (almost certain).

Unlikely (1)		**Possible (2)**		**Likely (3)**		**Almost certain (4)**	
Frequency[10]	Probability	Frequency	Probability	Frequency	Probability	Frequency	Probability
Occurs every 50 years or more	Less than 30% chance of occurrence over the period considered	Occurs every 15 - 50 years	30%-60% chance of occurrence over the period considered	Occurs every 3 - 15 years	60% - 90% chance of occurrence over the period considered	Occurs once or more every 3 years	Greater than 90% chance of occurrence over the period considered

[10] Frequency is a function of historic events while probability is a function of prediction for evaluating the likelihood of occurrence of harm. Using the concept of frequency or probability depends on the nature of the risk considered. Probability is more adapted when there are specific individual characteristics to be considered. Frequency is more adapted when the events are likely to be recurrent and/or it is not possible to make specific considerations.

APPENDIX 2: RISK IMPACT SCORING

To determine the impact of an event, should it occur, the possible types of impact (Programme delivery, Reputation, Finance, Human Resources, Ability to operate) should be kept in mind. Descriptors have been formulated for each type of impact; rates range from minor (1) to severe harm (4). These should be used as guidance to help with the assessment of impact scoring.

	Minor (1)	**Moderate (2)**	**Major (3)**	**Severe (4)**
Programme delivery Failure to deliver programme outputs (quantity and/or quality) and to achieve results as per the Programme and Budget document	Up to 15% reduction in scope and/or quality of intervention.	More than 15% and up to 30% reduction in scope or quality of intervention.	More than 30% and up to 60% reduction in scope or quality of intervention.	More than 60% reduction in scope or quality of intervention.
Reputation Lack of visibility, dissemination of incorrect information, information leaks, bad performance, unethical behaviour, etc.	Limited damage to the programme/CoE reputation. Minor one-off negative local publicity or visible dissatisfaction with the Programme by local stakeholder groups.	Some negative publicity or short-term damage to the programme/CoE reputation at a country-wide level resulting in loss of beneficiaries' confidence in the programme/CoE processes.	Negative publicity or damage to the programme's reputation at a national or state level resulting in ministerial inquiry, Director-General involvement, possible review of the administration of government, disruption to major departmental services or loss of public confidence in the department.	Significant and sustained negative publicity or damage to the Programme/CoE reputation at a global or national level resulting in senior staff resignations/ removals, inquiries or significant long-term damage to public confidence in the organisation. The organisation's mission or the conduct by an organisational leader is questioned.
Financial Loss Excess costs, shortfalls in income, procurement issues, financial losses, etc.	Affects up to 15% of the budget of the Programme	Affects more than 15% and up to 30% of the budget of the Programme	Affects more than 30 and up to 60% of the budget of the Programme	Affects more than 60% of the budget of the Programme
Human Resources Lack of motivation, frustration, conflicts, resignation, dismissal…	Affects up to 15% of Programme Staff	Affects more than 15% and up to 30% of Programme Staff	Affects more than 30% and up to 60% of Programme Staff	Affects more than 60% of Programme Staff
Ability to operate Breakdown of IT system, financial system…	Affects the ability of Programme to operate for up to 10 working days	Affects the ability of Programme to operate for more than 10 and up to 15 working days	Affects the ability of Programme to operate for more than 15 and up to 30 working days	Affects the ability of Programme to operate for more than 30 working days

APPENDIX 3: RISK EXPOSURE

The Combined effect of Impact and Likelihood defines the level of **Exposure** (Impact multiplied by Likelihood = Exposure). Each risk must be assessed keeping in mind the five types of possible impact proposed in Appendix 2 (Programme delivery, Reputation, Financial Loss, Human Resources, Ability to operate).

For each risk identified, exposures can be plotted on a Risk Matrix (see hereafter).

Example of RISK MATRIX	Minor (1)	Moderate (2)	Major (3)	Severe (4)
Almost certain (4)	4	8	12	16
Likely (3)	3	6	9	12
Possible (2)	2	4	6	8
Unlikely (1)	1	2	3	4

Depending on the level of exposures, different follow-up is recommended:

0 – 4 – Light - Green

Low risk exposure: the risk represents no immediate threat or impact and does not require much attention but should be reviewed at least once per year by the Programme Coordinator.

5 – 9 – Medium – Orange

Medium risk exposure: the risk has the potential to move to red. It needs managing and close monitoring but there is no immediate threat which would have a significant impact. It should be monitored and reviewed twice per year at a minimum by the Programme Coordinator.

10 – 16 – High - Red

High risk exposure: the risk requires active management. It poses an immediate threat and its impact could be significant. It should be constantly monitored and reviewed quarterly or monthly, if necessary. These are the 'top risks' of the programme. At organisational level **all risks within this score range will be considered by the Risk Management Working Group and in the intervening period will be monitored by the relevant Commitment Officers/Risk Focal Points**.

APPENDIX 4: OPERATIONAL RISK REGISTER – TEMPLATE

Risk register

Date	
Programme	
Risk Owner	The risk Owner is the is the senior manager who has responsibility for all risks within their programme.

RISK IDENTIFICATION		RISK ASSESSMENT TAKING INTO ACCOUNT MITIGATING ACTIONS ALREADY IN PLACE							RISK MITIGATION					Review	
Risk Category	Risk description	Likelihood			Impact			Exposure	Risk Manager	Mitigating Actions already in place	Additional measures planned to mitigate identified risks	Person responsible for implementing planned additional mitigating Actions	Deadline for additional mitigating actions to be in place	Review Date	Review Text
		Key			Key			Key							
Categorise the type of risk using the drop-down menu. Help with Risk Categories	Describe the risk in a narrative form: Source (cause) - As a result of.... Risk (uncertain event) - an event may occur.... Impacts (consequence) - which would lead to.....	4	Almost Certain	Greater than 90% chance of occurrence	4	Severe	Catastrophic adverse effects on operations, assets, or individuals	Overall Exposure rating = Likelihood x Impact 10-16 = High = RED 5-9 = Medium = ORANGE 0-4 = Low = GREEN	The Risk Manager is designated by the Risk Owner and is responsible for monitoring the evolution of the risk and the implementation of the mitigating actions. There should only be one Risk Manager for each risk	Identify the existing mitigating actions that reduce the exposure to the risk. Existing mitigating actions already have an effect on the assessment of the overall risk exposure. They need to be monitored to ensure that they remain in place. e.g. If a staff member who carries out a particular internal control leave s the department the controls should still be carried out by somebody else/their replacement	Identify additional mitigating actions aimed at -reducing the overall exposure relating to the Risk to the Target level. Additional mitigating actions should be designed to reduce the overall risk exposure to the Target level - mostly by reducing the likelihood of an event occuring.	The person responsible for implementing mitigating actions is designated by the Risk Manager. There should only be one person for each action	Each proposed mitigating action should have a deadline attached to it.	Set a date for the next review of the risk - the timeframe will depend upon the nature of the risk and the timeframe defined for the mitigating actions	Provide a brief summary of the evolution of the risk and the status of the mitigating actions
		3	Likely	More than 60% and up to 90% chance of occurrence	3	Major	Serious adverse effects on operations, assets, or individuals								
		2	Possible	More than 30% and up to 60% chance of occurrence	2	Moderate	Some adverse effects on operations, assets, or individuals expected								
		1	Unlikely	Up to 30% chance of occurrence	1	Minor	Limited adverse effects on operations, assets, or individuals expected								
Help	Help	Help			Help			Help							
								0							
								0							
								0							
								0							
								0							
								0							
								0							
								0							