Risk Management in DFID

Introduction

1. Risk management is important: it enables DFID to be innovative and to avoid disasters. But, like all management, it has to be done well. Unfortunately there is no universal guide, but there are approaches which improve risk management and tools to help.

2. Risk management is simple. The principles are to:
   - Think logically
   - Identify the key risks
   - Identify what to do about each risk
   - Decide who is responsible for actions
   - Record the risk and changes in risk
   - Monitor and learn

3. HM Treasury provides very good guidance on their website, although this is mainly aimed at UK activities. The website is: Treasury Risk Guidance

4. Risk is managed at three levels within DFID: **corporate, operational unit and intervention level.** This guidance covers the principles of risk management at all levels and the processes used to complete corporate and operational plan risk registers. The Management Board is responsible for the Corporate Risk Register (CRR) and this is updated quarterly. The purpose of the Operational Plan Risk Register is to highlight key risks at a lower level which require additional action or oversight. Collation of operational plan level risk also helps to inform corporate level risks and provides a mechanism to evaluate risks and determine whether risks may need escalated.

5. Risk affects all areas of DFID's work and there are many areas which require specialist knowledge and skills:
   - Security: people, IT
   - Health and safety
   - Civil contingency (protecting the public)
   - Business continuity
   - Scenario planning and political risk
   - Fiduciary risk
   - Internal financial controls
   - Aid impact and effectiveness
   - Disaster risk reduction

   There are specialists dealing with each of these areas and their support should be sought when needed.

Risk Management

6. Risk is defined as uncertainty, whether positive or negative, that will affect the outcome of an activity or intervention. The term 'management of risk' incorporates all the activities required to identify and control the exposure

to risk that may have an impact on the achievement of an organisation's business objectives.

7. Risk management is a key part of good management. The analysis of risk is an essential part of the design of any activity, whether large or small, internal and narrowly focused, or multi-partnered and global in impact. Many risk management activities already take part across DFID, but improvements need to be made to make these activities more visible and make the management of risk more explicit.

Risk Identification and Analysis

8. Risk rating analysis is the identification and evaluation of all risks to achieving objectives. The task of risk management is to limit the organisation's exposure to an acceptable level of risk in relation to the expected gain by taking action to reduce the probability of the risk occurring and its likely impact.

9. One of the difficulties of considering and evaluating risk is that different types of risk arise, which may not be easily comparable. However, it helps to identify the range of different types of risk involved. The list is open-ended, but examples are:
   - Development risk – project fails to result in poverty reduction
   - Delivery risk – outputs not achieved
   - Security risks – unsafe for DFID staff and partners to operate
   - Resource management risks – financial controls inadequate
   - Resource management risks – insufficient skilled staff available
   - Partner risks – partners not committed to the project objectives
   - Partner risks – partners' financial systems not sufficiently robust
   - Partner risks – partners have insufficient skilled staff available
   - Partner risks – political changes would affect the project negatively
   - Reputational risks – cross-cutting risks not fully addressed (gender, environment, climate change)
   - Reputational risks – certain groups oppose the project (particularly civil society or faith groups)
   - Reputational risks – failure would attract UK headlines
   - Reputational risks – a scandal with a partner would attract UK headlines

10. Risk analysis is subjective. In addition risks do not tend to have linear effects: but like the one small rock that starts an avalanche, one source of risk may give rise to several effects, or conversely there may be several sources of any particular effect. The overall impact of the whole portfolio of risks may be greater than the sum of the individual risks and should be considered as a whole. The range of risks that an organisation is exposing itself to should be considered on a regular basis to ensure that there is a well-judged balance between ambition and achievement (for example by ensuring that not everything is high risk).

11. Risk ratings are useful to managers as a relative, rather than absolute indicator, which will help to identify the most critical risks to success so that management effort can be prioritised. With a team of stakeholders

and partners the key risks to the objectives, viability or cost of the programme or activity should be identified. For each risk the impact of the risk and its probability should be estimated. Corporate and operational plan risk is rated on a 5 point scale (see tables 1 and 2). Intervention risk is rated on a 3 point scale (see tables 4 and 5). The results of this assessment can be presented in a risk rating matrix (table 3 for Corporate and Operational Plan risk and table 6 for intervention risk) which illustrates the overall distribution of risk.

Table 1

Probability for Corporate and Operational Plan risk

Traffic Light	Assessment	Interpretation
High	Is **expected** to occur, almost certain.	**Greater than 80%**
Medium/High	**Will** probably occur, measures may or may not exist to reduce likelihood.	**Between 20 and 80%**
Medium	**Could** occur, this is possible. Measures to reduce likelihood exist, but may not be fully effective.	**Between 10 and 20%**
Low/Medium	**Might** occur at some point in time. Conditions do exist for this to occur, but controls exist and are effective.	**Between 5 and 10%**
Low	Rare, **may** occur in exceptional circumstances. No or little experience for a similar failure;	**Less than 5%**

Table 2

Impact for Corporate and Operational Plan risk

Grade of Impact	Description	Interpretation
High	May cause key objectives to fail. Very **significant** impact on organisational goals. Legal or regulatory implications. Significant reputational impact.	Significant impact on MDGs. Significant impact on country programme. Significant impact on staff safety Financial implications exceed £40m
Medium/High	**Major effect.** Risk factor may lead to significant delays or non achievement of objectives.	Impact on country level objectives/ programme. Financial implications.
Medium	**Moderate** effect. Risk factor may lead to delays or increase in cost.	Considerable impact for programme/project. Financial implications
Low/Medium	Some impact of the risk, **fairly minor**.	Some impact for

		programme/project Financial implications
Low	**Fairly insignificant**, may lead to a tolerable delay in the achievement of objectives or minor reduction in Quality/Quantity/ and/or an increase in cost.	Financial implications

Table 3 Risk rating matrix for Corporate and Operational Plan risk

Probability						
Impact		**Low**	**Low/Medium**	**Medium**	**Medium/High**	**High**
	High	**High Impact** **Low Probability**	**High Impact** **Low/Medium Probability**	**High Impact** **Medium Probability**	**High Impact** **Medium/High Probability**	**High Impact** **High Probability** **"KILLER RISK"**
	Medium/ High	**Medium/ High Impact** **Low Probability**	**Medium/ High Impact** **Low/Medium Probability**	**Medium/ High Impact** **Medium Probability**	**Medium/ High Impact** **Medium/High Probability**	**Medium/ High Impact** **High Probability** **"KILLER RISK"**
	Medium	**Medium Impact** **Low Probability**	**Medium Impact** **Low/Medium Probability**	**Medium Impact** **Medium Probability**	**Medium Impact** **Medium/High Probability**	**Medium Impact** **High Probability**
	Low/ Medium	**Low/Medium Impact** **Low Probability**	**Low/Medium Impact** **Low/Medium Probability**	**Low/Medium Impact** **Medium Probability**	**Low/Medium Impact** **Medium/High Probability**	**Low/Medium Impact** **High Probability**
	Low	**Low Impact** **Low Probability**	**Low Impact** **Low/Medium Probability**	**Low Impact** **Medium Probability**	**Low Impact** **Medium/High Probability**	**Low Impact** **High Probability**

Table 4 Probability for Intervention risk

High	Very likely to occur and DFID's ability to actively manage the risk is limited.
Medium	Could go either way and DFID can have some influence in managing the risk but cannot control it completely.
Low	Unlikely to occur or the risk is fully manageable by DFID.

Table 5 Impact for Intervention risk

High	Risk factor may lead to considerable impact on the achievement of the Results as set out in the project log frame, for example results not being achieved, in relation to Time, Quality/Quantity to an acceptable standard or to an acceptable cost.
Medium	Risk factor may lead to moderate impact on the achievement of the Results in the log frame, for example in relation to time and/or loss of quality/quantity or to an acceptable cost.
Low	Risk factor may lead to no or only tolerable delay in the achievement of Results in the log frame or minor reduction in Quality/Quantity or to an acceptable cost.

Table 6 Risk rating matrix for Intervention risk

IMPACT ↑	**PROBABILITY** → **Low**	**Medium**	**High**
High	**High Impact** **Low Probability**	**High Impact** **Medium Probability**	**High Impact** **High Probability** **KILLER RISK!**
Medium	**Medium Impact** **Low Probability**	**Medium Impact** **Medium Probability**	**Medium Impact** **High Probability**
Low	**Low Impact** **Low Probability**	**Low Impact** **Medium Probability**	**Low Impact** **High Probability**

12. The risk rating matrix illustrates a hierarchy of risks at different levels. It allows consideration of how to respond to the identified risks and definition of any counter-measures especially to those risks that are most likely to impede success. All risks evaluated as high probability and high or medium/high impact should be addressed as 'killer risks'. These risks are very likely to occur and will have a significant impact on the achievement

of the Results in the project log frame (outputs, outcome and impact) or objectives at the operational unit level and ultimately costs.

Responding to Risk

13. Risk management responses can be a mix of five main actions; transfer, tolerate, treat, terminate or take the opportunity.

- **Transfer**; for some risks, the best response may be to transfer them. This might be done by conventional insurance or by supporting a third party to take the risk in another way.
- **Tolerate**; the ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. This course of action is common for large external risks. In these cases the response may be toleration but the risk should be tracked so managers are ready to reconsider should it start to escalate. Tolerance levels determining how much risk can be taken at each level need to be set and should inform your decisions.
- **Treat**; by far the greater number of risks will belong to this category. The purpose of taking action to reduce the chance of the risk occurring is not necessarily to obviate the risk, but to contain it to an acceptable level. Risk will be passed up and down the corporate chain. High-level risks may have to pass to a higher level of responsibility to decide on an action, whereas other risks may translate into activities designed to mitigate them. Decide what criteria will result in the risk being passed up the corporate management system.
- **Terminate** the risk by doing things differently thus removing the risk where it is feasible to do so.

14. Risk management should provide extra value to DFID. This means, for instance, that managers should:
    - Only take risks where there are likely to be benefits from doing so;
    - Focus management on risks where benefits could be enhanced, or the likelihood of success could be improved, or the likelihood of negative impact reduced;
    - Ensure that risk management is having an impact – and change it if it is not doing so.
    - Be proportionate – more attention may be appropriate for larger interventions.

Managing Individual Risks

15. A useful format to help analyse and record individual risks has been developed for the CRR (annex 1) with a simpler format for Operational Plan Risk Registers (annex 2).

16. Risk management should add value to DFID, so the main issue is whether the mitigating actions make a difference. The format is to help guide analysis and planning to make sure the actions are well targeted and effective. It is intended that this is only used for the most significant risks. Generally the advice is to focus on four or five main threats depending on the size and complexity of the area at risk/intervention.

17. There are broadly six areas: the description of the risk, the triggers, inherent/residual rating of the risk, the mitigating actions, direction of travel, and whether the residual risk is within the Management Board appetite for risk in that area.

Description of the risk

18. Risks should be worded to clearly identify what the cause and effect of the risk is. A good place to begin is considering what the objective is and then thinking about the potential risks. This aims to make clear what the consequences of a risk are. It requires judgement to set the level of description, but it should indicate what is important to DFID.

19. There is a tendency for us all to talk in general terms – for instance the risk of having a car crash. But the crash itself isn't the issue; it is the consequences in terms of injuries, damage to the car, financial loss, and temporary lack of transport which matter. In a car crash the first priority is about personal injury, so the risk could be describe as "risk of a car crash resulting in life threatening injury or injury requiring more than one week off work". There is a judgement on the level of detail, but normally all the consequences are not needed (cost of bandages, time taken seeing the doctor etc) – just concentrate on the major effect of the risk. The description should specify all of the key elements of the risk, since the response to each (mitigating actions) may be different. Risks should be worded in such a way to remove any ambiguity.

Triggers

20. Triggers are early warning signals which should indicate in advance if a risk is likely to occur. Using the car crash example, this might be that the car fails the MOT. Or that the driver has worked too hard and is very tired. Or that there's mud on the road. If a trigger point is reached or imminent then it is necessary to review and possibly to take action or change approach. The proximity to some triggers may be influenced by mitigating actions, however, it is acceptable to have triggers which we have no control over and which are simply an indication that we are edging nearer to the risk being realised.

Inherent/Residual Risk

21. **Inherent risk** is the level of risk occurring in the absence of any actions management has taken to alter either the risk's impact or probability. Where risk responses (mitigating actions and existing controls) have been developed these should be identified. **Residual risk** is the rating given to

the risk after action has been taken to alter the risk's impact and probability.

22. Effective risk management requires that the responses (mitigating actions) selected are proportionate to the risk being managed and the most efficient way of reducing the residual risk to manage the risk in line with DFID's risk appetite for that particular risk area. By measuring both the inherent and residual risks, more informed decisions can be taken regarding the optimum level of risk and mitigating actions. Risk management used in this manner can be used to focus limited resources on the key risk areas.

23. Unless there is no possible response to the risk we would expect to see a change in risk rating between the inherent risk value and the residual risk value. If there is no change and residual risk is rates the same as inherent risk it may be necessary to consider the effectiveness of the mitigating actions and whether or not they are the right mitigating actions.

The mitigating actions

24. The mitigating actions are the key to the risk management. They should focus on the risk as a whole and should be actions which make it less likely that a risk will occur, or which reduce its impact, probability or both. They may, as a side benefit, reduce the likelihood of triggers being reached however the triggers should not be the main focus. They should be as Specific Measurable Achievable Realistic and Time bound (SMART) as possible. There is a requirement to measure progress with mitigating actions and to highlight to management where mitigating actions are off track. If the mitigating action is an on-going, recurrent action/control, consideration should be given whether this needs to be reported in the risk register.

25. For the car crash example, some actions could be: check the tyres; service the car regularly; don't drink and drive; travel by train; live on Colon say. For DFID, examples might be:
    - get monthly project accounts to avoid the risk of major financial fraud (reduces probability);
    - draft contingency plans and staff training on what to do in an earthquake (reduces impact);
    - hold regular reviews of progress on IT projects to identify emerging problems (reduces probability and impact);
    - Make training on Freedom of Information and Copyright mandatory (reduces probability and impact).

26. Mitigating actions which stay the same over a long period should be reviewed as they may not be effective, although they might still be necessary.

Direction of travel

27. It can be helpful to consider what possible events may occur in the near future which can impact on your assessment of risk. This can also help to focus your mitigating actions. Three options are provided to indicate the direction of travel; these are increasing, static or decreasing.

Risk Appetite

28. Risk appetite is defined as the 'amount of risk to which the organisation is prepared to accept, tolerate, or be exposed to at any point in time '[1] i.e. limiting exposure to an acceptable level for the expected gains by identifying the amount of risk that can be tolerated. The Management Board have produced a statement of DFID's risk appetite to provide direction on risk appetite and set the boundaries for risk management in DFID. This provides clear guidelines to staff to indicate where risks can be taken and where they cannot.

29. DFID has a high risk appetite when it comes to taking risks to achieve our key targets. The Management Board states:

    DFID has a **high** risk appetite to invest in research opportunities which support the creation of new evidence where these have the potential to have practical use at an operational level.

    But a lower risk appetite in relation to staff safety and security and fiduciary risk. The Management Board states:

    DFID is not willing to intentionally risk the security of its personnel and assets or accept weak financial management.

30. Risks should be managed to within the Management Boards appetite for risk in that area. Where the residual risk is well below the appetite for risk in that area this may indicate that a disproportionate amount of resources (e.g. staff time or funds) are being used to mitigate that risk. This would allow you to free up this resource for redeployment elsewhere.

31. Generally, risks that have been mitigated down to within the Management Board's risk appetite would be tolerated. Additional management action to treat, transfer or terminate the risk would normally only come in to play if the residual risk was above the risk appetite.

32. Overall, risk registers allow managers to see what risks are being tackled and whether any progress is being made. They can then decide whether to continue as before, add more resources, or escalate the risk up the management chain.

33. The format adopts the principle of risk owners, an approach recommended by the Office of Government Commerce. Risk owners take prime responsibility for managing and reporting on key risks. Annex 3 gives an overview of Management Board responsibility for risk and suggested terms

[1] HM Treasury Orange book

of reference to risk owners at different levels of DFID. Annexes 5 and 6 give guidance on completing risk registers at corporate and operational plan levels.

Annex 1 – CRR format

Risk X

Restricted

Specific Risk		**Risk Area**	
		Owner	
		Monitor	
		Co-ordinator	

Triggers & Proximity to triggers	**1**		**Please Select**
	2		**Please Select**
	3		**Please Select**
	4		**Please Select**
	5		**Please Select**

Probability and Impact Assessment on Inherent Risk	
Probability	**Please Select**
Impact	**Please Select**

Mitigating Actions	**1**		**Please Select**
	2		**Please Select**
	3		**Please Select**
	4		**Please Select**
	5		**Please Select**

Probability and Impact Assessment on Residual Risk	
Probability	**Please Select**
Impact	**Please Select**

Direction of Travel	**Please Select**

Risk Appetite for this risk is **xxxx.** Is the risk remaining after mitigating actions within the stated risk appetite?	**Please Select**

Management Action	**Please Select**

Please comment on the current status of the risk - including off track mitigating actions, any additional mitigating actions proposed, the direction of travel of the risk and proposed actions if residual risk assessment is out- with risk appetite.

Annex 2
Operational Plan Risk Register Format

No/ Category	***Risk Description***	***Triggers***	***Mitigating Actions***	***Residual Probability***	***Residual Impact***	***Direction of Travel***[2]	***Within Risk Appetite?***	***Management Actions***[3]	***Owner***
Risk 1									
Risk 2									
Risk 3									
Risk 4									
Risk 5									

[2] Direction of travel is an indication of whether the residual risk is **increasing, decreasing** or remaining **static,** talking account of possible events in the near future which may impact in the assessment of the risk.
[3]Management Actions are: **Treat, transfer, tolerate** or **terminate**

2
3

Annex 3

Management Board responsibility for risk and suggested Terms of Reference for Risk Owners;

Objective of these Terms of Reference

The objective of these terms of reference is to clearly set out the responsibilities of the Management Board and risk owners at different levels of corporate management, so that these can be discussed, agreed, communicated to colleagues and understood across the organisation. To be effective risk ownership must be clearly defined, documented and agreed with the individual owners at all levels. This enables them to understand their various roles, responsibilities and ultimate accountability with regard to the management of risk. A further aim is to help clarify what responsibility can be taken for risk management at different corporate levels and when risks and responsibilities for them should be passed up the system to a higher level.

Responsibility at board level

1. Take the risk challenge function role within the organisation so that it is clear that risk is taken seriously and that top management see this as an important issue.
2. Identify the risks that will prevent DFID from delivering its Structural Reform Plan (SRP) targets by agreeing and reviewing the CRR.
3. Check key interdependent risks that cross organisational boundaries.
4. Take responsibility for setting DFID's risk appetite for specific areas of risk.
5. Regularly consider the range of risks that the organisation is exposing itself to, to ensure that there is a well-judged balance between ambition and achievement (for example by ensuring that not everything we do is high risk). Challenge each other's view and management of risk.
6. Ensure that the effectiveness of DFID's risk policy management is evaluated and quality assured on a regular basis.
7. When appropriate delegate risks downwards.
8. Ensure consistency across the Organisation in the ways that risks are evaluated and mitigated.

Proposed TORS for Risk Owners at CRR level

1. Lead in defining the risk management framework for the organisation and ensure that all staff see risk as a key aspect of delivery management.
2. Identify the risks that will prevent the organisation from reaching its Structural Reform Plan targets
3. Ensure a suitable monitor is identified for the risk.
4. Evaluate the risks (impact and probability) and ensure that this is regularly updated as circumstances change.
5. Mitigate the inherent risk to within the Management Boards appetite for risk in that area.
6. Identify suitable responses to risk (tracking or management) and implement these should risks escalate.
7. Regularly review the risk strategy to assess the effectiveness of the management of risk processes.

Proposed TORS for Risk Owners at Operational Unit level

1. Identify the key risks to the achievement of Operational Plan objectives

2. Evaluate the impact and probability of the risks including identifying areas of high and low risk where more (or less) management input will be needed.
3. Set the acceptable levels of risk that the country office/operational unit can tolerate for each high level risk and clarify areas where risks can be taken and where they cannot.
4. Check the balance of the portfolio of challenge and risk. This will include tracking intervention risks (i.e. checking that all interventions are not high or low risk)
5. Identify and implement suitable responses to risk, including passing risk management upwards should the risk situation escalate.
6. Regular checking of key interdependent risks that cross organisational boundaries.

Proposed TORS for Risk Owners at intervention level

1. Identify the risks that will prevent or delay the intervention from achieving the expected results set out in the log frame, i.e. the outputs, outcome and Impact. .
2. Evaluate each of the risks to establish their impact and probability.
3. Use the evidence/evaluation data to risk score the intervention.
4. Manage the risks if and when they occur, including passing escalating risks up to Operational Unit level when appropriate.
5. Regularly review the risk strategy to assess the effectiveness of the management of risk processes and review the risk scoring of the intervention.

Annex 4

Corporate Risk Registers
When updating the CRR:

- Consider whether the risks are still valid;
- Ensure the risks are the "live" issues facing the Organisation;
- Identify any new risks to propose for inclusion, either as a result of escalation from Operational Unit level or entirely new;
- Review the trigger indicators and whether any circumstances have materialised which impact on the risk rating;
- Ensure the Risk Owner and Monitor are correctly identified;
- Ensure that the cause and effect of the risk are clearly identified;
- Assess the triggers and indicate whether each one is distant, imminent or has been reached;
- Provide probability and impact ratings for **inherent** risk;
- Review the mitigating actions to ensure that they are SMART, in particular, clearly identify a target date for each mitigating action;
- If the mitigating action is an ongoing control issue, consider rewording this to reflect any action you will be taking in relation to this;
- Only include key mitigating actions (ideally a maximum of 5)
- Indicate, using the drop down box, whether the mitigating action is on or off track;
- Provide probability and impact ratings for **residual;**
- Set **direction of travel** for each risk from the drop down list. This can either be increasing, static or reducing.
- Consider whether the risk remaining after mitigating actions is within the stated risk appetite and select any further management action;
- Complete a short narrative on the current status of the risk – including off-track mitigating action, direction of travel of the risk over the following 3 months and proposed action if residual risk is beyond risk appetite in that area;

Annex 5

Operational Plan Risk Registers
Guidance for completion

When updating the Operational Plan Risk Register:

- Consider if the risks are still valid,
- Consider if the risks are the “live” risks facing the Operational Unit,
- Are there are any new risks to include? (including significant risks from lower level risk registers);
- Are relevant Corporate risks are adequately reflected at Operational Unit level;
- Consider if the key reasons/risks for not achieving objectives are reflected in your risk register; and
- Identify any risks should be escalated to a corporate level.
- Ensure description and trigger indicators are up to date and valid.
- Assess the Probability and Impact of the residual risk using the five point scale.
- Critically review mitigating actions, consider whether these can be made time bound and ensure responsibilities are clear.

August 2011
Finance & Performance Department