Assessing risks and performing a risk analysis

We define risk as the likelihood of an incident occurring that negatively affects our operation. There may be risks that affect the organisations, the activities of the project or operation, and the possibility of achieving the goal.

Having a finely prepared strategy for risk management entails taking a preventative approach in your work, and having a solid contingency plan in the event that something should happen which affects the operation in an undesirable manner. Before finalising the planning of the operation, it is therefore necessary to conduct a risk analysis.

Carrying out a risk analysis involves determining the extent to which there is a risk of failing to achieve the stated goals as a result of internal or external circumstances, i.e. it entails you discussing what you can envisage might hinder or complicate the implementation. Enter the results of these discussions and how you grade the risks in the “Risk” section of the application, along with a description of your plans for dealing with the risks. You can then follow up on the risks as the operation is conducted, and the risk matrix should reappear in the report.

How do you perform a risk analysis?

The simplest way is to conduct it in the form of a brainstorming session, where potential risks and scenarios are aired and discussed. It is important to do this as a part of your work to plan the operation, and it should subsequently be followed up as the operation progresses, so as to keep it relevant.

A risk analysis consists of four different stages:

1. Identify the risks that exist.
2. Discuss the consequences to the organisation or the operation if any of the risks identified should occur.
3. Assess the likelihood of the risks occurring.
4. Prepare an action plan for what to do in the event that the risks occur, as well as how you can work to prevent these risks occurring. Then enter the risks in what is known as a **risk matrix** (see Figure 1).

A fundamental distinction should be made between **external** and **internal** risks. External risks are risks over which the organisation has no control (e.g. the political situation in the country, the attitudes of the local authorities, natural disasters and so on). Internal risks are risks that you as an organisation can influence directly. These could, for example, be the risk of exceeding the budget, inadequate administrative routines, conflicts within the working group, or key personnel leaving the organisation. Both external and internal risks must be observed in the risk analysis. The risk of corruption – both external and internal—must always be included in a risk management plan.

One helpful approach in this regard is to review various types of risk and discuss the situation in your organisations and working groups:

- **Disasters** (examples): Severe drought, armed conflicts, epidemic or pandemic.
- **Financial risks** (examples): Major change in exchange rates, bank crash, corruption at societal level or within the organisation. Break-in and theft at the office.
- **Staff risks** (examples): the project manager is not working full time on the project. The members of the project team are divided between different projects and/or working on other tasks. Someone has more than one role in the project. Internal disputes. Illness. Key personnel leave the organisation. Brain drain.
- **Legal risks** (examples): Problems registering the organisation. Difficulties obtaining various permits. Legal proceedings initiated against key personnel at the organisation. The organisation is not granted permits to carry out activities.
- **Security risks** (examples): The authorities impound the project/organisation material. Activities monitored by the authorities. No virus protection on the organisation's computers.
- **Organisational risks** (examples): Lack of support from the management and board, some skills not represented in the organisations.
Inadequate administrative routines. Inadequate internal democratic structures. Discrimination against certain groups.

Figure 1: Risk matrix

Risk	Consequence	Likelihood (high, medium, low)	Action plan
1. Key personnel leave the organisation	Important knowledge about the operation is lost	Medium	Make sure that multiple people within the organisation have access to the important knowledge by taking care to document in detail, by arranging training for more people in the organisation, and by ensuring hand-over.

You can download tools for calculating risk factors from our website under Method material.