RISK MANAGEMENT GUIDANCE

Introduction

BACK TO INDEX

We can't tell what will happen in the future – but we can often make a good guess at it!

If we don't do so, we simply have to react to what happens. By then, our options are limited and it's too late to influence events.

If we think of what might happen, we have the opportunity to take steps to change how likely it is or to change what the impact will be if it does happen.

This is the essence of risk management. It's a simple but effective way of making the future more like we'd want it to be.

What is a Risk?

BACK TO INDEX

A risk is defined as:

The **chance** of something **happening** that will have an **impact** on **objectives**.

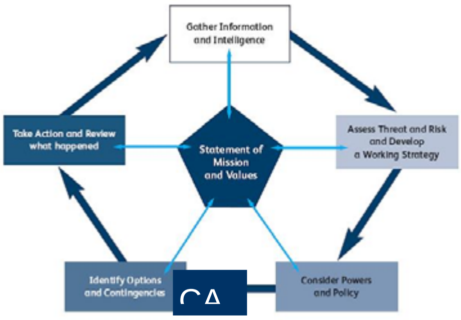
It is given a clear description and is assessed in terms of how likely it is to occur and the impact if it should occur, in other words the combination of the probability of an event and its consequences.

It should be noted that this applies to positive events (opportunities) as well as negative events (threats).

Risk Management in Practice

BACK TO INDEX

We must be aware of risks in order to have proper planning and decision-making, but risk management is not about trying to eliminate risks. There will always be risks, but if we can identify and assess them, then we can make a conscious choice to accept some risks and to take action in respect of others – but that action should be *proportionate*: if it does not deliver an *expectation of benefit*, why would we take it?


Gather Information and Intelligence
Assess Threat and Risk and Develop a Working Strategy
Consider Powers and Policy
Identify Options and Contingencies
Take Action and Review what happened
Statement of Mission and Values
CA

This concept is developed in the seven-step process which follows. This is very much on the same lines as the National Decision Model, used in operational service.

We need to ensure that the right level of risk is being considered at the right meetings across the organisation. The structure of the Portfolio Boards and the requirement to escalate risks (to them and also from them to the Risk & Harm Board) is designed to ensure that this is the case. (See Step 5 below)

Risk Management Process

BACK TO INDEX

There are seven steps to the risk management process:

1) ORIENTATION

BACK TO INDEX

Consider the team/dept/organisation in question and its objectives

It is necessary to "focus in" on your part of the organisation, to be clear about what the actual risk is and what it means for you.

Where there are risks which may apply more widely – to many parts of the organisation as a whole – these should be escalated for information. (See Step 5) One simple reason for this is that a solution which may not be viable locally may make perfect sense from the broader standpoint.

Where risks are identified which do not apply to your area, but which may be informative to others, they should be referred as suggestions to the relevant colleagues. (Sometimes useful insights are obtained from outside one's own area.)

2) IDENTIFICATION

BACK TO INDEX

Identify the risks which could affect achievement of those objectives and describe them clearly

Risks may be identified within the division under review or may be referred to it – from below (escalation), from above (delegation) or otherwise, as described under Step 1.

Where identifying risks directly, it can be very useful to get together a number of people from the division for a brainstorming session. To do this effectively, it is usually best to break down the possible risks into different areas, to facilitate ideas. One method of doing this is **PESTEL** (or PESTLE) which is a mnemonic for the categories of **P**olitical, **E**conomic, **S**ocial, **T**echnological, **E**nvironmental and **L**egal. (It is not really important under which category a given risk is considered – the important thing is to use the categories as a prompt to allow more risks to be identified.)

Once identified, risks which are to be taken forward should be carefully described, so that they are reasonably concise and yet can be understood by others. The preferred method of doing this is to use a three-part description, including the **Source(s)** of the risk, the **Event** itself which is being anticipated and the **Impact(s)** which would follow. Examples are given in the sample risk register attached as **Annex A**.

3) ASSESSMENT[1]

BACK TO INDEX

[1] Note that the Health & Safety Risk Assessment is a combined risk identification and risk assessment exercise, specifically for Health & safety related risks and there is a separate procedure and guidance for this. Note that it may be appropriate to conduct one or the other or both, depending on the circumstances.

Prioritise these risks, by assessing how likely they are to occur and the level of impact if they should occur

Consider the risk, as identified and described. Before assessing how likely it is to occur and the level of impact if it should occur, take account of existing control measures.

Take the opportunity to consider whether these control measures are actually in place and are still appropriate, or whether there is now a better way to respond.

Next, consider the risk as it now is – allowing for the existing controls, but not for any further changes which you may wish to make – and rate it for probability and impact. Guidance on how to do this – what selection to make from the five-point scale in each case – is given in **Annex B**. When these two selections are added to the risk register, under Step 6, the **Initial Risk Rating** will be produced, expressed as a numerical score and a colour of either green, amber or red. Clearly, at the outset of a new risk, this will also be the **Current Risk Rating**, which will automatically show on the register. That rating may be overwritten, as required, as the status of the risk develops. (One further assessment will follow later – the **Target Risk Rating**, discussed under Step 7.

4) OWNERSHIP

BACK TO INDEX

Each risk should be owned and managed by an appropriate person – usually the person who would have responsibility for the objective or area of work in any case

It is important to have an individual owner for a risk and normally it should be owned at the lowest level at which it can be properly managed, having regard to availability of resources, delegated authority etc. Any actions to be taken in respect of the risk can (and normally should) be owned by others.

Ownership of the risk may change following escalation or delegation. (See Step 5) This will normally be the case, but (a) risks may be escalated initially for information and the ownership may not transfer and (b) in the case of the transfer of a risk from one owner to another, this must be clearly accepted and recorded.

5) RESPONSE

BACK TO INDEX

Consider how to respond to each risk, which may vary from avoiding the activity altogether to doing nothing at all

There are four principal responses to a risk, as well as the possibility of transferring the risk upwards (escalation) or downwards (delegation). Each of these is described below.

The four principal responses are ACCEPT, AVOID, TREAT and TRANSFER.

ACCEPT – the risk is acknowledged, but does not need to be addressed or any action which could be taken in respect of the risk would be disproportionate. In any event, it is considered to be acceptable as it is. This position should be kept under occasional review, to ensure that this remains the case.

AVOID – the risk is not considered acceptable and there is no reasonable way to make it so, meaning that the best thing to do is to avoid this area of risk altogether. Note that, because of the nature of our work and the expectations upon us, this will often not be a viable option.

TREAT – this is the most common response to an identified risk and involves taking steps to modify the likelihood of occurrence (the probability) or the consequences if it should occur (the impact). Note that any action to be taken in respect of a risk will have resource implications and may also give rise to additional risks. Therefore, care should be exercised and actions should be taken only where there is the expectation of benefit overall. In other words, our response should be *proportionate*. (The use of the **Target Rating** section in the risk register assists with this and is designed to try to avoid unnecessary work.)

TRANSFER – the other possible response is to transfer all or part of the risk to someone else. An example of this would be a specialist contractor, for example for the removal of asbestos. Purchasing insurance cover transfers most of the financial consequences of specified events. However, it should be noted that it is not normally possible to transfer potential impact to our reputation.

ESCALATE – in accordance with the terms of reference of the Risk & Harm Board and the Portfolio Boards, "red" risks (and other significant risks) should be escalated to the next level up, at least for information. Apart from "red" risks, any risk should be escalated if there is not the authority or the resource to manage it effectively. A problem which seems intractable at one level may be solved at the next and it is extremely important that this opportunity is provided.

DELEGATE – Similarly, risks which can be properly managed at a lower level may be delegated. In any such case of change of ownership of a risk it is important that this is clearly communicated, accepted and recorded.

6) RECORD-KEEPING

BACK TO INDEX

Maintaining the risk register (and other documents it may refer to) to track decisions and actions

The risks register is not an end in itself – what really matters are the risks and how we manage them – but it is an important way of recording the risks, the decisions made about them, actions to be taken etc and of making this information available to colleagues.

a step-by-step guide as to how to complete the risk register is given in **Annex C**.

7) REVIEW

BACK TO INDEX

It is crucial to monitor and review and refine activity, to maintain a proportionate response and to learn from experience

There is no *correct* frequency for reviewing risks – it very much depends on the risk itself. Some risks may be regarded as being relatively static, but for others a review on a daily basis (or even more frequently) may be appropriate. A review on at least a monthly basis is recommended, but also risk owners should have a constant awareness to new developments. A risk may be reviewed and put away for a month, but the next day you may hear something on the radio or read something in a staff bulletin which means that risk needs to be revisited.

When a risks has reached its Target Rating, any actions taken in respect of it have become well embedded and it is not felt necessary to keep it under review on the risk register, then it may be archived.

Try to pick up learning points from this process wherever possible and use the guidance on learning lessons and the organisational learning matrix to share anything which you believe could be of benefit to colleagues.

Benefits of Risk Management

BACK TO INDEX

Risk management can help you track the things that are important, avoid problems (and time-consuming consequences) and generally work more effectively. In general, the benefits of risk management are:

to help make the right decisions for the right reasons

to contribute to the internal control framework

to reduce volatility and avoid surprises

to protect and optimise our resources

to protect and enhance our physical assets

to protect and develop our human assets

to improve stakeholder relationships

to protect and enhance our reputation

Comments/Feedback/Training Requests

BACK TO INDEX

The Management of Risk team is here to coordinate risk management work (including the specific areas of Business continuity, Health & Safety and Insurance) and to provide support and advice for all managers in the management of their risks.

We welcome any comments you may have, whether questions or feedback you wish to submit, requests for training or of any other nature. Please don't hesitate to contact us.