

# **MANAGEMENT OF RISK**

~ ~ ~ ~ ~

# **A STRATEGIC OVERVIEW**

~ ~ ~ ~ ~

*WITH SUPPLEMENTARY GUIDANCE FOR SMALLER BODIES*

---

**HM Treasury**  
**January 2001**

# CONTENTS

<b>Section</b>	<b>Description</b>	<b>Page</b>
1	Overview	2
2	The Strategic Risk Management Cycle	3
3	Identify The Risks And Define A Framework	4
4	Assign Ownership	6
5	Evaluate	7
6	Assess Risk Appetite	8
7	Response To Risk	9
8	Gain Assurance	12
9	Embed And Review	13
10	Glossary Of Key Terms	14
	<b>SUPPLEMENT FOR SMALLER BODIES</b>	15
S1	Introduction	16
S2	Approach	17
Annex	Proforma Risk Register	19

# 1. OVERVIEW

It is a matter of definition that the running of any organisation is primarily concerned with the achievement of objectives. The organisation exists for a purpose - perhaps to deliver a service, or to achieve particular outcomes. In the private sector the primary purpose of an organisation will generally be concerned with the enhancement of shareholder value; in the central government sector the purpose is generally concerned with the delivery of service or with the delivery of a beneficial outcome in the public interest. Whatever the purpose may be, its achievement will face all manner of risks.

The task of management is to respond to these risks so as to maximise the likelihood of achieving the purpose. The resources available for doing so are finite and so the aim is to achieve an optimum response to risk, prioritised in accordance with an evaluation of the risks. Some amount of risk taking is necessary – the only way to avoid risk is to do nothing at all which is guaranteed to ensure that nothing is achieved. Managers therefore need to be equipped with skills and tools which allow them to have a reasonable assurance of achieving their objectives with reasonable value for money.

The essence of risk is the uncertainty of outcome (whether positive or negative). The term **exposure** refers to the combination of the **probability** of these potential events and the magnitude of their **impact**.

- **Probability:** the evaluated probability of a particular outcome actually happening (including a consideration of the frequency with which the outcome may arise)
- **Impact:** the evaluated effect or result of a particular outcome actually happening

The task of **risk management** is the **management of this exposure** to an acceptable level, by taking action on probability, impact (or both); it therefore requires identification of the elements to be considered, not all of which may be controllable.

Risk can be thought of as arising in two ways:

- direct **threats** (damaging events) which could lead to failure to achieve objectives, and
- **opportunities** (constructive events) which if exploited could offer an improved way of achieving objectives but which are surrounded by threats.

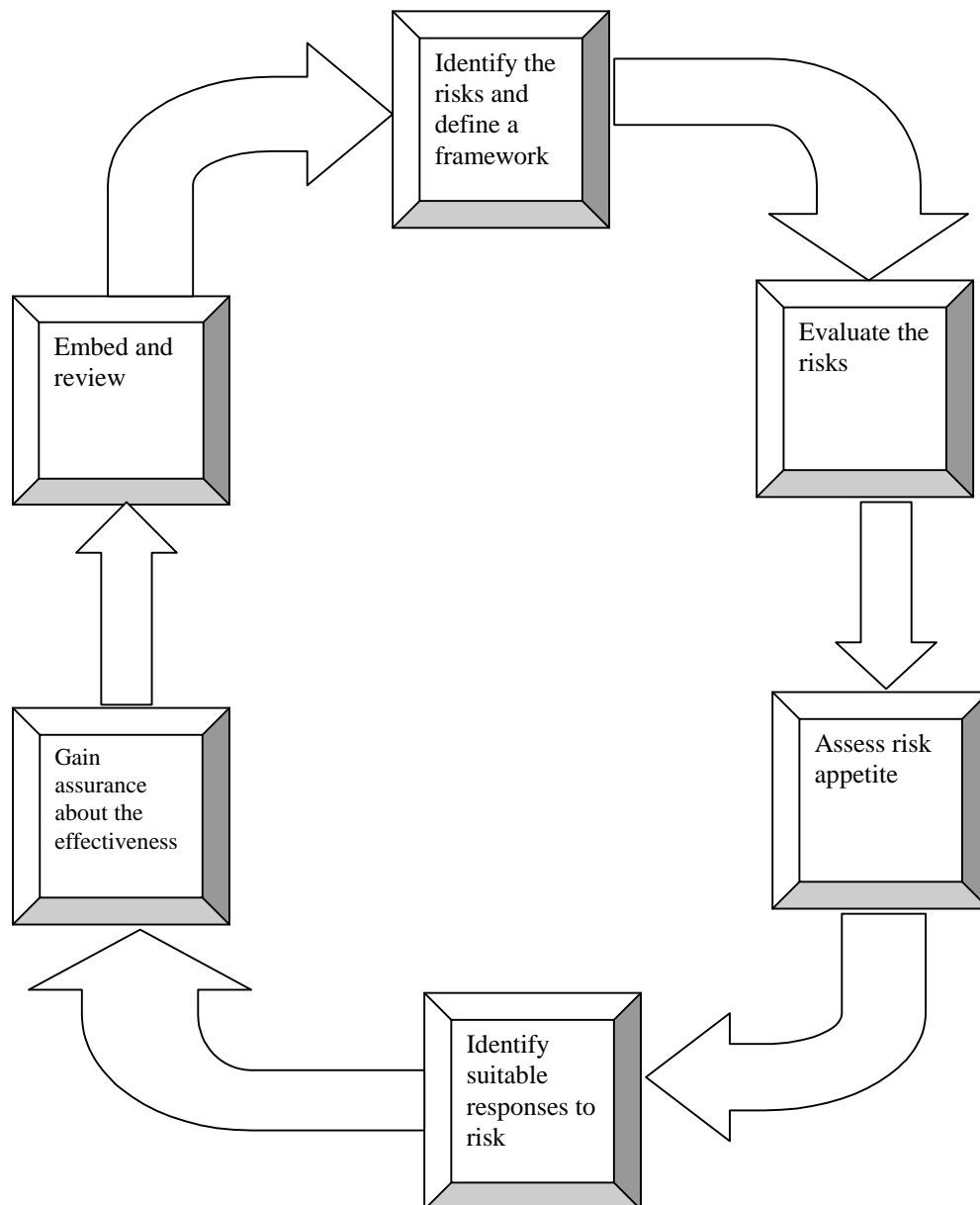
In either case an organisation needs to put in place a corporate and consistent strategy for handling risk in order to ensure that it has an agreed and understood methodology for achieving its objectives.

Numerous detailed documents already exist giving guidance on risk management in general circumstances (for example the “Green Book”) and in particular circumstances (such as the guidance for PFI projects). This guide does **not** aim to offer a single solution to the challenge of risk management, nor does it attempt to tell the reader how to manage risk. That would not be possible as the detail of risk issues for any one organisation is particular to that organisation, and to that organisation alone.

This guide **does** aim to offer - as its title implies - some pointers to developing a strategic framework for the organisational consideration of risk. It points towards some tools and techniques which may be adopted by an organisation as it considers the adequacy of its risk management processes across the whole range of risks which have to be dealt with in the course of its day to day business.

## 2. THE STRATEGIC RISK MANAGEMENT CYCLE

There is a continuous “cycle” to the risk management process:



Each element of the cycle is described in more detail in the following sections.

## 3. IDENTIFY THE RISKS AND DEFINE A FRAMEWORK

*There are three important principles for analysing risk:*

- *adopt a consistent approach throughout the organization*
- *ensure that there is a clear structure to the process so that each element or level of risk identification fits into an overall structure*
- *establish a framework, approved at senior level, within which risk is to be identified.*

*A strategic approach to risk management depends on identifying risks against key organisational objectives. Organisations that have already built risk frameworks in this way have found that it is most practical to confine the objectives at this level to a small number, certainly not exceeding ten. Risks relevant to these objectives are then considered and evaluated allowing a small number of key risks to be identified.*

### 3.1 RISK IDENTIFICATION TOOLS

It is necessary to adopt an appropriate tool for the identification of risk. Two of the most commonly used tools are:

Commissioning a risk review: A designated team is established (either in-house or contracted in) to consider all the operations and activities of the organisation in relation to its objectives and to identify the associated risks. The team should work by conducting a series of interviews with key staff at all level of the organisation to build a risk profile for the whole range of activities.

Risk self assessment: A bottom up approach by which each level and part of the organisation is invited to review its activities and to feed upwards its diagnosis of the risks faced. This may be done through a documentation approach (with a framework for diagnosis set out through questionnaires) or through a facilitated workshop approach (with facilitators with appropriate skills helping groups of staff to work out the risks affecting their areas of responsibility)

These approaches are not mutually exclusive and a combination of top down and bottom up inputs to the risk assessment process is desirable.

### 3.2 CATEGORIES OF RISK

One of the difficulties of considering and evaluating risk is that different types of risk arise, which may not be easily comparable. However, a critical stage in any attempt to evaluate risks is to identify the range of different types of risk involved. It may be helpful to consider risks either as primarily arising from some source or as leading to an effect. However, most risks contain elements of both.

The table below offers a summary of the most common categories of risk with examples of the nature of the source and effect issues. The table does not claim to be comprehensive - some organisations may be able to identify other categories of risk applicable to their work.

<b>CATEGORY OF RISK</b>	
<b>External</b>	
1. Infrastructure	Relating to infrastructures such as transport systems for staff, power supply systems, suppliers, business relationships with partners, dependency on internet and e-mail
2. Economic	Relating to economic factors such as interest rates, exchange rates, inflation
3. Legal and Regulatory	Relating to the laws and regulations which if complied with should reduce hazards (Eg – Health and Safety at Work Act)
4. Environmental	Relating to issues such as fuel consumption, pollution
5. Political	Relating to possible political constraints such as change of government
6. Market	Relating to issues such as competition and supply of goods
7. “Act of God”	Relating to issues such as fire, flood, earthquake.
<b>Financial</b>	
8. Budgetary	Relating to the availability of resources or the allocation of resources
9. Fraud or theft	Relating to the unproductive loss of resources
10. Insurable	Relating to potential areas of loss which can be insured against
11. Capital investment	Relating to the making of appropriate investment decisions
12. Liability	Relating to the right to sue or to be sued in certain circumstances
<b>Activity</b>	
13. Policy	Relating to the appropriateness and quality of policy decisions
14. Operational	Relating to the procedures employed to achieve particular objectives
15. Information	Relating to the adequacy of information which is used for decision making
16. Reputational	Relating to the public reputation of the organization and consequent effects
17. Transferable	Relating to risks which may be transferred or to transfer of risks at inappropriate cost
18. Technological	Relating to the use of technology to achieve objectives
19. Project	Relating to project planning and management procedures
20. Innovation	Relating to the exploitation of opportunities to make gains
<b>Human Resources</b>	
21. Personnel	Relating to the availability and retention of suitable staff
22. Health and Safety	Relating to the well-being of people

## 4. ASSIGN OWNERSHIP

*The importance of identifying key risks is not only to identify the most important areas to which resource should be allocated in risk management but also to allocate responsibility for management of these risks.*

### 4.1 THE IMPORTANCE OF ASSIGNING OWNERSHIP

The most effective risk management emerges when ownership of any particular key risk is allocated to an appropriate senior official; without ownership being assigned at a senior level responsibility and authority for implementing control actions is unlikely to be clear. Accounting Officers, of course, have to remain personally accountable for their organisations and for its risk management; however a framework of senior level delegation is essential if risk management is to be effective.

### 4.2 CO-ORDINATION OF RISK OWNERSHIP

There are various means by which the delegation framework can be established.

- \* The designated risk owners can be formed into a “Risk Management Committee” which reports to the Accounting Officer or acts as a sub-committee to the senior management Board
- \* Where there is a Board structure to senior management it may be helpful to allocate risk ownership to Board members and to put risk management on the Board Agenda on a regular basis
- \* Where there is a strong representation of senior managers on the Audit Committee it may be helpful to allocate risk ownership to executive members of the Audit Committee, and to ask the Audit Committee to regularly consider risk management issues.

The important issue is not the detail of the process, but the principle that a senior structure of ownership of risk is established. It is also important that

- \* whatever senior level structure is adopted, a mechanism for reporting to the Accounting Officer (who has to retain ultimate responsibility) on risk issues is established
- \* Risk owners recognize that their participation in any form of committee structure does not diminish their personal responsibilities for the risks assigned to them

## 5. EVALUATE

*In order to decide how to handle risk it is essential not only to identify the principle that a certain type of risk exists, but to evaluate its significance. To achieve this a consistent identification tool has to operate within the evaluation framework. One of the key purposes of risk evaluation is to inform decisions about the areas of risk in which action needs to be taken and their relative priority; consequently consistency in the evaluation is important.*

### 5.1 PRINCIPLES OF EVALUATION

Some types of risk lend themselves to a numerical diagnosis - particularly financial risk. For other risks - for example reputational risk - a much more subjective view is all that is possible. In this sense risk evaluation is more of an art than a science. It will be necessary, however, to develop some framework for categorising risks as (say) high / medium / low. Generally it will be better to minimise the categories, as over refinement may lead to fallacious separation of levels of risk which in reality cannot be clearly segregated. A management judgement on the extent to which levels of any particular type of risk can be separated will be required .

### 5.2 THE USE OF MODELS

The evaluation of individual risks at various levels should be carried out using a model for the comparison of the results. It will be necessary to build a model (often done using spreadsheets) which facilitates the processing and amalgamation of the evaluation to provide an overview of the overall risk profile. The building of a risk model, like the categorisation of risk, involves subjective judgement both in the input to the model and in the interpretation of results. Experience with such models shows that if the results appear odd to those who are familiar with the organisation and its work, an iterative process of adjustment be required before an acceptable result is obtained. This is not pre-judging or undue influence on the model; it is simply a reflection of the fact that risk evaluation is an art, and management of risk is judgmental rather than mechanistic.

A variety of risk models can be procured “off the shelf”. When developing a model for a particular organisation it is important to recognize (particularly in central government) that each organisation is established for a unique purpose and the model used has to be appropriate to that organisation. “Off the shelf” models, or models copied from other organisations can only offer a starting point for developing the “right” model for the particular organisation. Specific tailoring of any models procured from external sources will inevitably be required.

## 6. ASSESS RISK APPETITE

*An important issue in considering response to risk is the identification of the “risk appetite” of the organisation<sup>1</sup>.*

### 6.1 DEFINING “RISK APPETITE”

Risk appetite is the amount of risk to which the organisation is prepared to be exposed before it judges action to be necessary. Even risk as opportunity is surrounded by threats which potentially limit ability to exploit the opportunity, and for which an appetite in relation to the opportunity benefit has to be assessed. The fact that the resources available to control risks are likely to be limited means that value for money decisions have to be made – what resource cost is it appropriate to incur to achieve a certain level of control in respect of the risk? Apart from the most extreme circumstances it is unusual for good value for money to be obtained from any particular risk being completely obviated with total certainty.

Risk appetite may be very specific in relation to a particular risk, or it may be more generic in the sense that the total risks which an organisation is prepared to accept at any one time will have a limit.

### 6.2 FEATURES OF IDENTIFYING THE RISK APPETITE

In consequence every organisation has to identify its risk appetite. Decisions about response to risk have to be taken in conjunction with an identification of the amount of risk that can be tolerated. Any particular organisation is unlikely to have a single risk appetite. The tolerable extent of risk will vary according to the perceived importance of particular risks. For example, tolerable financial loss may vary in accordance with a range of features including the size of the relevant budget, the source of the loss, or associated other risks such as adverse publicity. Where a particular risk can give rise to a number of effects, an effect of quite large financial loss may be acceptable whilst an associated effect of damage to health and safety may not be tolerable at all. Both the risk framework, and the control responses, therefore have to be considered in detail to identify the appropriate balance of potential realization of risk against the costs of limiting that risk.

The most significant issue is that it is unlikely, except for the most extreme risks, that any particular risk will need to be completely and absolutely obviated. Identification of risk appetite is a subjective (rather than an objective or scientific) issue but nevertheless is an important stage in formulating the overall risk strategy.

---

<sup>1</sup> The “Green Book” (Appraisal and Evaluation in Central Government) offers detailed advice on appraising benefits in relation to options and opportunities.

## 7. RESPONSE TO RISK

*The result of the actions outlined above will be a risk profile for the organisation. Having developed a risk profile, consideration can then be given to appropriate response.*

### 7.1 RISK RESPONSES

Responses to risk can be divided into four response categories:

- TRANSFER :** For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. In essence,
- TOLERATE :** 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. In these cases the response may be toleration.
- TREAT :** By far the greater number of risks will belong to this category. The purpose of treatment is not necessarily to obviate the risk, but more likely to contain the risk to an acceptable level. The actions that an organisation takes in treating risk are called “internal control” - they are actions instigated from within the organisation (although their effects may be felt outside of the organisation) which are designed to contain risk to acceptable levels.
- TERMINATE:** Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities may be severely limited in government when compared to the private sector; a number of activities are conducted in the government sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can be achieved.

### 7.2 DEFINING INTERNAL CONTROL

“Control” is any action, procedure or operation undertaken by management to increase the likelihood that activities and procedures achieve their objectives. Control is therefore a response to risk - it is intended to contain uncertainty of outcome that has been identified. The term “internal control” is sometimes used - this indicates that the origin of the control is within the organisation and distinguishes management action from external control such as that imposed by external regulatory bodies.

### 7.3 CATEGORIES OF INTERNAL CONTROL

Internal controls can be classified in four ways:

- DETECTIVE CONTROLS:** These controls are designed to identify occasions of undesirable outcomes having been realised. Their effect is, by definition, “after the event” so they are only appropriate when it is possible to accept the loss or damage incurred. Examples of detective controls include stock or asset checks (which detect whether stocks or assets have been removed without authorisation), reconciliation (which can detect unauthorised transactions), and “Post Implementation Reviews” which detect lessons to be learnt from projects for application in future work.
- DIRECTIVE CONTROLS :** These controls are designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided - typically associated with Health and Safety or with security. Examples of this type of control would be include a requirement that protective clothing be worn during the performance of dangerous duties, or that staff be trained with required skills before being allowed to work unsupervised.
- PREVENTIVE CONTROLS :** These controls are designed to limit the possibility of an undesirable outcome being realised. The more important it is that an undesirable outcome should not arise, the more important it becomes to implement appropriate preventive controls. The majority of controls implemented in organisations tend to belong to this category. Examples of preventive controls include separation of duty, whereby no one person has authority to act without the consent of another (such as the person who authorises payment of an invoice being separate from the person who ordered goods prevents one person securing goods at public expense for their own benefit), or limitation of action to authorised persons (such as only those suitably trained and authorised being permitted to handle media enquiries prevents inappropriate comment being made to the press).

**CORRECTIVE CONTROLS :** These controls are designed to correct undesirable outcomes which have been realised. They provide a route of recourse to achieve some recovery against loss or damage. An example of this would be design of contract terms to allow recovery of overpayment. Insurance can also be regarded as a form of corrective control as it facilitates financial recovery against the realisation of a risk.

#### **7.4 PROPORTIONALITY OF CONTROL**

In designing control, it is important that the control put in place is proportional to the risk. Apart from the most extreme undesirable outcome (such as loss of human life) it is normally sufficient to design control to give a **reasonable assurance** of confining likely loss within the risk appetite of the organisation. Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling. Generally speaking the purpose of control is to **contain** risk rather than to **obviate** it.

## 8. GAIN ASSURANCE

*A risk management framework having been developed, and a control response having been implemented, it is essential that assurance about the effectiveness of these actions is obtained.*

### 8.1 REPORTING

The first mechanism to be implemented to assist with gaining assurance is a reporting system. This allows the management structure to report upwards about how risk management is being effected. This reporting system should be owned by, and report to, the Accounting Officer through whatever mechanisms have been established for the co-ordination of risk ownership.

Two particular tools can be considered :

- \* If CRSA is adopted, is that the results of each CRSA exercise are considered by the body of risk owners, who can then report in turn to the Accounting officer.
- \* “Stewardship Reporting” requires that designated managers at various levels of the organisation report upwards (usually at least annually at the financial year end, and often on a quarterly or half yearly interim basis) on the work they have done to keep risk and control procedures up to date and appropriate to circumstances within their particular area of responsibility.

### 8.2 INTERNAL AUDIT

Every central government organisation is required to make provision for Internal Audit. Internal Audit’s work will provide an important assurance about the adequacy of management’s embedded risk and control mechanism.

Internal audit may be used by management as an expert internal consultant to assist with the development of a strategic risk management process for the organisation. It will have a wide ranging view of the whole range of activities which the organisation undertakes, and will already have undertaken some form of assessment to inform its planning of systems and processes to be audited. However it is important to note that the function of Internal Audit is to give **independent** assurance about the way in which risk is controlled; it is neither a substitute for management ownership of risk nor is the presence or activity of Internal Audit a substitute for an embedded review system carried out by the various staff who have executive responsibility for the achievement of organisational objectives.

### 8.3 OTHER REVIEW BODIES

Many organisations may have specialist review and assurance teams which have been established for a particular purpose (for example, Accounts Inspection Teams, or Compliance Review Teams). Their work contributes to the assurances available about the risk and control systems in use in the organisation.

## **9. EMBED AND REVIEW**

*It is important to remember that the risk environment of any organisation is constantly changing, and priorities of objectives and the consequent importance of risks will shift and change. Risk models have to be regularly revisited and reconsidered in order to have assurance that the risk profile continues to be valid.*

### **9.1 EMBEDDING THE STRATEGY**

The objectives of an organization should be hierarchical. In an organization the objectives of directorates / divisions / teams / individuals will be related to the organisation's top level objectives. Risk management demands that appropriate awareness of, and responsibility for, risk issues lies in parallel with the structure of objectives. At every level of objectives there should be a parallel delegation of responsibility for the associated risk issues. This is critical to embedding risk management into the structure of the organisation. The embedding of risk management is in turn critical to its success; it should become an intrinsic part of the way the organisation works, at the core of the management approach; not something separated from the day to day activities.

### **9.2 KEEPING THE RISK STRATEGY UP TO DATE**

It has already been noted that the risk environment of any organisation is constantly changing and developing, and that the priorities of objectives and the consequent importance of risks will shift and change. The risk management process is therefore a dynamic and ongoing one, not an issue for a "one off" exercise. The process has to allow for periodic review of risks and for consequent adjustment of the control response.

The principle of "Corporate Governance" requirements is to ensure that the risk and control structure embedded into the organisation is subjected to review by senior management.

A number of options for the senior level ownership and control of the process have been offered in this guide. Whatever option is adopted, it is important that those charged with control of the risk management process regularly review it. One useful technique for doing this is to actively review the risks associated with each of the key organisational objectives (on a cyclical basis, the whole cycle being contained within a year to meet corporate governance requirements).

### **9.3 TOOLS FOR KEEPING THE STRATEGY UP TO DATE**

Suitable tools need to be identified to assist with the task of keeping the risk strategy up to date. A key tool is the use of ongoing Control and Risk Self Assessment (CRSA) procedures. This procedure embeds review of risk and control into the organisation at every level and uses the knowledge and experience of the staff that are closest to each function to assess the movement in risks and the appropriateness of control.

## 10. GLOSSARY OF KEY TERMS

Assurance	gaining (independent) confirmation that risk assessment and control response is appropriate, adequate and achieving the effects for which it has been designed
Control	any action, procedure or operation undertaken to either contain a risk to an acceptable level of potential exposure or to increase the probability of a desirable outcome
Corrective control	a control designed to correct undesirable outcomes
Detective control	a control designed to detect undesirable outcomes which have arisen
Directive control	a control designed to ensure a particular outcome
Embedding risk management	ensuring that the risk management strategy is reflected in the objectives and function of every level of the organisation
Exposure	the range of outcome arising from the combination of the impact of an event and the probability of the event actually happening
Impact	the evaluated effect or result of a particular outcome actually happening
Opportunity	an uncertainty of outcome that may result in a positive or beneficial impact that the organisation wishes to take advantage of or exploit.
Preventive control	a control designed to prevent an undesirable happening
Probability	the evaluated probability of a particular outcome actually happening (including a consideration of the frequency with which the outcome may arise)
Risk	the uncertainty of outcome, within a range of exposure, arising from a combination of the impact and probability of potential events.
Risk appetite	the range of exposure that is judged tolerable for the organisation
Risk management	the limitation of the exposure to an acceptable level, by taking action on probability, impact (or both); it therefore requires identification of the elements to be considered and which may be controllable. A model of this is offered below:
Risk review	a strategic review sponsored by senior management to identify the risks associated with all the activities and operations of the organisation.
Risk self assessment	a technique by which each level of the organisation identifies and evaluates the risks associated with its activities to inform a strategic review
Threat	an uncertainty of outcome likely to result in a negative or damaging impact that the organisation may wish to control to an acceptable level.

**SUPPLEMENT**

**FOR**

**SMALLER BODIES**

## S1. INTRODUCTION

The guidance in the main text of this book is designed to primarily be of use to larger bodies with a complex system of control based on a broad management structure, it may not be so appropriate for smaller bodies where the system of internal control is relatively straight forward, and where there are relatively few members of staff, with multiple responsibilities. In these instances, the indivisibility of the available resources may have implications for the strategic framework.

The risk management process is equally important in a small body as in a large department. However, it is necessary to develop an approach that is appropriate to the particular circumstances of small bodies. With these considerations in mind, this supplementary guidance aims to assist smaller bodies develop a suitable approach to risk management

This guidance does not attempt to define what is a “smaller body”, but, as indicated above, presumes two key characteristics of such bodies:

- a less complicated system of internal control due to limited diversity of risk; and
- a limited number of staff carrying out multiple functions.

This guidance does not, in any way, reduce the Corporate Governance requirements placed on those bodies thought to be “small”, it merely serves to provide guidance on an approach to the risk management process that is more appropriate to their size.

Our suggested approach assumes that day to day control of the body is restricted to a small board- style management group, who are well aware of, and involved in, the various functions of the body and the activities being undertaken. The approach requires the management board to invest a certain amount of time at inception in order to lay the foundations for the ongoing risk management process.

The key starting point for the process is the strategic objectives of the organisation, as it is the risks to the achievement of these objectives on which the body should focus attention. If the body does not have an agreed set of strategic objectives, then the development of these will need to be the first stage of this process. Ideally, looking forward, risk management should be embedded into the ongoing planning and strategy process. It is up to the individual organisation to judge the significance of the risks they face and how much attention to give them.

## S2. THE APPROACH

### *Stage 1 - preparation*

Given the nature of the internal control system and the particular pressure on available resources in small bodies, this approach aims to keep the time input required to a minimum. The main text of this book proposes a series of risk management workshops as a means of identifying and assessing the risks. For small bodies we suggest that one meeting of the senior officers within the organisation should suffice although some preparation will be required prior to the meeting. It is also important to decide upon an appropriate individual within the organisation to take overall control of the risk management process and to chair the risk meeting. This is most likely to be a senior member of the management team whose role affords a global overview of the activities of the body.

Prior to the meeting, the objectives of the body should be circulated to all attendees with a request for them to consider, and then submit, what they perceive to be the risks to achieving each of those objectives. In order to share ownership of the process throughout the organisation, attendees may wish to consult other members of staff at this stage. As a guide, it may be useful to send participants the list of potential categories of risk at Section 3 of the main text.

From the submissions received, and using his/her judgement, the Chairman should then aim to arrive at an overall list (grouping as appropriate) of the main risks facing the organisation.

### *Stage 2 – the meeting*

The objectives of the risk meeting are as follows:

- Discuss and agree that all involved are satisfied with the Chairman's list of risks;
- Determine the appropriate response to each risk;
- Assess existing controls and determine appropriate action;
- Allocate responsibility for action; and
- Agree future reporting and review procedures.

Taking each of the risks in turn, discuss and rate them high/medium/low in terms of likelihood and impact.

With this exercise complete, the Board needs to decide what their risk appetite is (see section 6 of main text). This will determine what response the board wishes to make to each risk. For details of the different possible responses to risk see Section 7 of the main text.

With the list of key risks and responses agreed, it is then time to identify any controls that already exist in relation to the risks. The controls identified need to be assessed to determine whether they are an *appropriate* response to of the risks identified. The value for money of the chosen responses needs to be considered: over-control of minor risks is as important to avoid as under-control of serious risks.

It is likely that the assessment of controls will produce a list of actions required to produce an acceptable internal control system. Clear responsibilities should be allocated to these actions along with a deadline for the action to be completed and a scheduled date for review.

### ***Stage 3 – the risk register***

Following the meeting, the risk register proforma can be completed (see Annex ). At this point, it may be sensible to circulate it to other relevant members of the organisation who did not attend the meeting. They should be able to provide further confirmation that the understanding of the risks and controls within the organisation is accurate.

A final version of the register should be circulated to all members of the organisation so that they are aware of the risk management policy and the controls in place to limit exposure to risk.

For some organisations, a formal risk register may not be the most appropriate means of tracking the risks over time, and other less formal means of reporting on how they are managed may already exist within the management and planning processes of the body. Organisations should ensure that the risk assessment is embedded into the management and planning processes and not carried out as an isolated exercise. The risk register, or equivalent, should provide valuable input to the allocation of resources, in order to help factor risk into the business planning processes.

### ***Stage 4 – ongoing review and reporting mechanisms***

Management should agree a timetable for continuing review of the risk register, bearing in mind that the key risks faced by the organisation may change and that the adequacy of the internal control system requires regular re-assessment.

**ANNEX TO SUPPLEMENT FOR SMALLER BODIES**

**PROFORMA RISK REGISTER**

<b>Risk</b>	<b>Likelihood / Impact</b>	<b>Response</b>	<b>Control;</b>	<b>Accept? (y.n)</b>	<b>Action required</b>	<b>By whom</b>	<b>Action by (date)</b>	<b>Next review date</b>
<i>Inadequate staff cover</i>	<i>High/high</i>	<i>Treat</i>	<i>Planning, scheduling/rotas.</i>	<i>y</i>	<i>None.</i>	<i>N/a</i>	<i>N/a</i>	<i>3/01</i>
<i>Theft of key exhibits</i>	<i>High/high</i>	<i>Treat</i>	<i>24 hour security presence, CCTV, staff screening</i>	<i>y</i>	<i>Regular review of effectiveness of controls</i>	<i>AN Other</i>	<i>12/00</i>	<i>2/01</i>
<i>Ability to access museum without ticket</i>	<i>High/med</i>	<i>Treat</i>	<i>Ticket office at front door manned by one person at all times</i>	<i>n</i>	<i>Cost/benefit analysis of installation of gates at front door, securing all other points of access, having extra staff at front door.</i>	<i>AN Other</i>	<i>11/00</i>	<i>1/01</i>
<i>Failure to attract visitors</i>	<i>Med/high</i>	<i>Treat</i>	<i>Management review of attendance figures, visitor feedback questionnaires</i>	<i>y</i>	<i>Regular review of effectiveness of controls</i>	<i>AN Other</i>	<i>12/00</i>	<i>3/01</i>

N.B. The entries in the risk register are for **illustration** only – to provide an indication of the responses required in each column.