

# **“THE ORANGE BOOK”**

*(Revised Version)*

## **MANAGEMENT OF RISK**

*Principles and Concepts*

**CONSULTATION DRAFT**

**May 2004**

**HM Treasury**

*Assurance, Control  
And Risk Team*

# CONTENTS

| <b>Section</b> |  | <b>Page</b> |
|----------------|--|-------------|
| 1              | Foreword                               | 2           |
| 2              | Overview                               | 3           |
| 3              | The Risk Management Model              | 5           |
| 4              | Identifying risks                      | 6           |
| 5              | Assessing risks                        | 9           |
| 6              | Addressing risks                       | 11          |
| 7              | Reviewing and reporting risks          | 14          |
| 8              | Communication and learning             | 16          |
| 9              | The Extended Enterprise                | 18          |
| 10             | Risk environment and context           | 19          |
| 11             | Risk appetite                          | 20          |
| Annex 1        | Example of documenting risk assessment | 21          |
| Annex 2        | Overall assurance on risk management   | 22          |
| Annex 3        | Summary of horizon scanning issues     | 25          |
| Annex 4        | Glossary of key terms                  | 26          |

# 1. FOREWORD

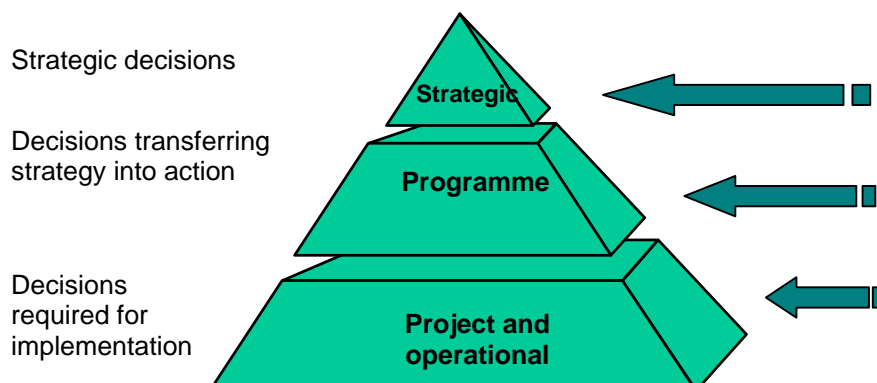
- 1.1 In recent years all sectors of the economy have focused on management of risk as the key to making organisations successful in delivering their objectives whilst protecting the interests of their stakeholders. In central government a number of reports, particularly the National Audit Office’s 2000 report “Supporting innovation – managing risk in government departments”, and the Strategy Unit 2002 report “Risk – improving government’s capacity to handle risk and uncertainty” have driven forward the risk management agenda along with the development of Statements on Internal Control.
- 1.2 In 2001 Treasury produced “Management of Risk – A Strategic Overview” which rapidly became known as the Orange Book. That publication provided a basic introduction to the concepts of risk management which proved very popular as a resource for developing and implementing risk management processes in government organisations. This publication is the successor to the 2001 “Orange Book” – it continues to provide broad based general guidance on the principles of risk management and whilst retaining the same basic principles has been enhanced to reflect the lessons we have all been learning about risk management through the experience of the last few years. It should be read and used in conjunction with other relevant advice such as the “Green Book” which contains specific advice on “Appraisal and Evaluation in Central Government” and the Office of Government Commerce’s “Management of Risk” which provides more detailed guidance on the practical application of the principles and concepts contained in this publication.
- 1.3 Perhaps the most significant shift since the publication of the 2001 “Orange Book” is that it can now be presumed that all existing organisations have basic risk management processes in place. This means that the main risk management challenge does not lie in the initial identification and analysis of risk and the development of the risk management process, but in the ongoing review and improvement of the risk management process. This guidance aims to reflect that – for instance, it now includes guidance on issues such as “horizon scanning” for change in risk. Never the less, sufficient guidance on developing risk management “from scratch” has been retained to ensure that the guidance is useful in newly created organisations which do have to develop their processes from the beginning. This guidance also aims to not just focus on the internal processes for risk management but to also offer support in considering the organisation’s risk management in relation to the wider environment in which the organisation functions.
- 1.4 This guidance should be useful to both those who are experienced in risk management who will find it a useful baseline against which to review their processes and to those who are new to risk management who should find it helpful in introducing the concepts. It will also be equally of use whether the reader’s focus of interest is with managing risk at strategic, programme or operational levels.

HM Treasury  
May 2004

## 2. OVERVIEW

- 2.1 It is a matter of definition that organisations exist 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 of the organisation may be, the delivery of its objectives will be surrounded by uncertainty which both poses threats to success and offers opportunity for increasing success.
- 2.2 Risk is defined as this uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. The risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen. Risk management includes identifying and assessing risks (the “inherent risk”) and then responding to them.
- 2.3 The resources available for managing risk 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. The amount of risk which is judged to be tolerable and justifiable is the “risk appetite”.
- 2.4 Response, which is initiated within the organisation, to risk is called “internal control” and may involve one or more of the following: to decide to tolerate the risk, to transfer the risk, to terminate the activity giving rise to the risk, to treat the risk in an appropriate way to constrain the risk to an acceptable level or actively taking advantage, regarding the uncertainty as an opportunity to gain a benefit. The level of risk remaining after internal control has been exercised (the “residual risk”) is the *exposure* in respect of that risk, and should be acceptable and justifiable – it should be within the risk appetite. Risk management processes should be embedded into the routine planning and operational systems of the body and all staff should be appropriately trained to manage risk relevant to their particular responsibilities.
- 2.5 None of this takes place in a vacuum. Every organisation functions within an environment which both influences the risks faced and provides a context within which risk has to be managed. Further, every organisation has partners on which it depends in the delivery of its objectives whether they be simply suppliers of goods which the organisation requires or direct partners in the delivery of objectives.
- 2.6 All of this means that an organisation which wants to maximize its success in delivering its objectives needs to have a risk management strategy, led from the very top of the organisation, which is then implemented by managers at every level of the organisation in the particular activities which they manage, and embedded in the normal working routines and activities of the organisation. The management of risk at strategic, programme and operational levels needs to be integrated so that the levels of activity support each other.

Figure 2.1 Hierarchy of risk



Acknowledgements: SU report *Risk: improving government's capability to handle risk and uncertainty*, Nov 2002

- 2.7 Managers at every level therefore need to be equipped with appropriate skills which will allow them to manage risk effectively and the organisation as a whole needs a means of being assured that risk management is being implemented in an appropriate way at every level. Every organisation should have a risk management strategy, designed to achieve the principles set out in this publication, which is documented, approved by the Accounting Officer / Board, promulgated throughout the organisation, and regularly reviewed to provide assurance that it remains effective and appropriate.
- 2.8 This guide aims to provide an introduction to the range of considerations which apply in risk management, all of which can be applied at various levels ranging from the development of a strategic, organisation-wide risk policy through to management of a particular project or operation. It does so using a risk management model which is set out in the next section – each element of the model is explored in further detail. The guide focuses firstly on the “lifecycle” core of the model, then gives consideration to the wider based issues which form the overall risk management environment. It is important to note that this guide is *not* a detailed instruction manual for how to manage risk – its aim is simply to draw attention to the range of issues which are involved and to offer some general direction to help the reader think about how these issues may be addressed in the specific circumstances of their own organisation.
- 2.9 There is not a specific agreed standard for risk management in government organisations. This guide establishes principles of risk management, and the “Risk Management Assessment Framework”<sup>1</sup> provides a means of assessing the maturity of risk management. Organisations may choose to adopt particular standards (for example, the Australian standard<sup>2</sup>, AIRMIC<sup>3</sup>, or Coso<sup>4</sup>), but the critical thing to aim for is ability to demonstrate that risk is managed in the particular organisation, in its particular circumstances, in a way which achieves the risk management targets which the organisation has set for itself to effectively support the delivery of objectives.

<sup>1</sup> [http://www.hm-treasury.gov.uk/media/7B1D9/risk\\_management\\_assessment\\_070104.pdf](http://www.hm-treasury.gov.uk/media/7B1D9/risk_management_assessment_070104.pdf)

<sup>2</sup> <http://www.riskmanagement.com.au/>

<sup>3</sup> <http://www.airmic.com>

<sup>4</sup> [http://www.erm.coso.org/Coso/coserm.nsf/vwWebResources/PDF\\_Manuscript/\\$file/COSO\\_Manuscript.pdf](http://www.erm.coso.org/Coso/coserm.nsf/vwWebResources/PDF_Manuscript/$file/COSO_Manuscript.pdf)

### 3. THE RISK MANAGEMENT MODEL

Notes on the model

- The management of risk is not a linear process; rather it is the balancing of a number of interwoven elements which interact with each other and which have to be in balance with each other if risk management is to be effective. Furthermore, specific risks cannot be addressed in isolation from each other; the management of one risk may have an impact on another, or management actions which are effective in controlling more than one risk simultaneously may be achievable.

- The whole model has to function in an environment in

which risk appetite has been defined. The concept of risk appetite (how much risk is tolerable and justifiable) can be regarded as an “overlay” across the whole of this model.

- The model presented here, by necessity, dissects the core risk management process into elements for illustrative purposes but in reality they blend together. In addition, the particular stage in the process which one may be at for any particular risk will not necessarily be the same for all risks.

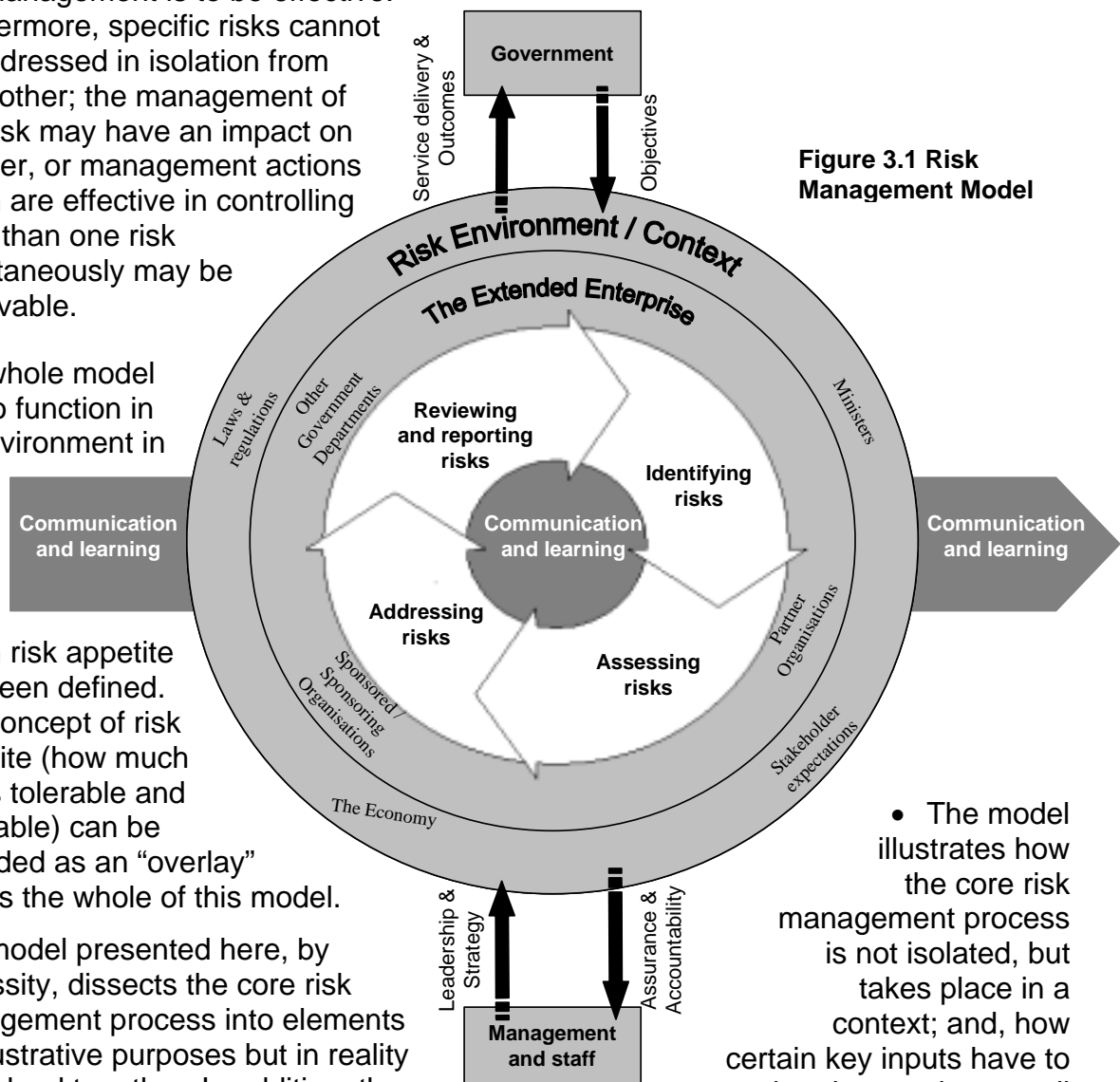


Figure 3.1 Risk Management Model

- The model illustrates how the core risk management process is not isolated, but takes place in a context; and, how certain key inputs have to be given to the overall process in order to generate the outputs which will be desired from risk management.

## 4. IDENTIFYING RISKS



- 4.1 In order to manage risk, an organisation needs to know what risks it faces, and to evaluate them. Identifying risks is the first step in building the organisation’s risk profile. There is no single right way to document an organisation’s risk profile, but documentation is critical to effective management of risk.
- 4.2 The identification of risk can be separated into two distinct phases. There is:
- initial risk identification (for an organisation which has not previously identified its risks in a structured way, or for a new organisation, or perhaps for a new project or activity within an organisation), and there is
  - continuous risk identification which is necessary to identify new risks which did not previously arise, changes in existing risks, or risks which did exist ceasing to be relevant to the organisation.
- 4.3 In either case risks should be related to objectives. Risks can only be assessed and prioritised in relation to objectives. When a risk is identified it may be relevant to more than one of the organisation’s objectives, its potential impact may vary in relation to different objectives, and the best way of addressing the risk may be different in relation to different objectives (although it is also possible that a single treatment may adequately address the risk in relation to more than one objective). In stating risks, care should be taken to avoid stating impacts which may arise as being the risks themselves, and to avoid stating risks which do not impact on objectives; equally care should be taken to avoid defining risks with statements which are simply the converse of the objectives. A statement of a risk should encompass the cause of the impact, and the impact to the objective which might arise

|   |   |
|---|---|
| <b>Objective</b> – to travel from A to B for a meeting at a certain time          |   |
| Failure to get from A to B on time for the meeting                                | <b>X</b> this is simply the converse of the objective   |
| Being late and missing the meeting  | <b>X</b> This is a statement of the impact of the risk, not the risk itself                                 |
| There is no buffet on the train so I get hungry                                   | <b>X</b> this does not impact on achievement of the objective   |
| Missing the train causes me to be late and miss the meeting                       | <b>✓</b> This is a risk which can be controlled by making sure I allow plenty of time to get to the station |
| Severe weather prevents the train from running and me from getting to the meeting | <b>✓</b> This is a risk which I cannot control, but against which I can make a contingency plan             |

- 4.4 Typically a larger organisation will find that it identifies a large number of risks in total – perhaps several hundred. These risks will not all be independent of each other; rather they will typically form natural groupings. For instance, there may be a number of risks which can be grouped together as “financial risks” and further risks which can be grouped together as “Human Resource risks”. These groupings of risks will incorporate related risks at strategic, programme and operational levels (see 2.6). It is important not to confuse a grouping of risks with the risks themselves. Risks should be identified at a level where a specific impact can be identified and a specific action or actions to address the risk can be identified. All risks, once

identified, should be assigned to an owner. A risk owner, in line with their accountability for managing the risk, should have sufficient authority to commit resources to addressing the risk; the risk owner may not be the person who actually takes the action to address the risk.

- 4.5 It is necessary to adopt an appropriate approach or tool for the identification of risk. Two of the most commonly used approaches 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 levels of the organisation to build a risk profile for the whole range of activities.
  - Risk self-assessment: An approach by which each level and part of the organisation is invited to review its activities and to contribute its diagnosis of the risks it faces. This may be done through a documentation approach (with a framework for diagnosis set out through questionnaires), but is more commonly conducted through a facilitated workshop approach (with facilitators with appropriate skills helping groups of staff to work out the risks affecting their areas of responsibility)
- 4.6 These approaches are not mutually exclusive, and a combination of approaches to the risk assessment process is desirable – this sometimes exposes significant differences in risk perception within the organisation. These differences in perception need to be addressed to achieve effective integration of risk management at the various levels of the organisation.
- 4.7 Horizon scanning activities are increasing both in public and private sectors as the importance of early warning of risk developments, giving time for the preparation of effective response strategies, is increasingly appreciated. There can be considerable variation between organisations in their approach to horizon scanning because of differing organisational needs. A summary of horizon scanning issues, provided by the Civil Contingencies secretariat of the Cabinet Office is at Annex 3.
- 4.8 The table on the next page offers a summary of the most common categories or groupings of risk with examples of the nature of the source and effect issues; it is intended to help organisations ensure that they have comprehensively considered the range of potential risk which may arise; it also provides headings under which organisations may choose to group their specific risks in their risk profile documentation. The table does not claim to be comprehensive - some organisations may be able to identify other categories of risk applicable to their work.

| CATEGORY OF RISK  | Examples / explanation  |
|---|---|
| <b>1. External (arising from the external environment, not wholly within the organisation’s control, but where action can be taken to mitigate the risk)</b><br><i>[This analysis is based on the “PESTLE” model – see the Strategy Survival Guide at <a href="http://www.strategy.gov.uk">www.strategy.gov.uk</a>]</i> |   |
| 1.1 Political   | Change of government, cross cutting policy decisions (Eg – the Euro); machinery of government changes   |
| 1.2 Economic  | Ability to attract and retain staff in the labour market; exchange rates affect costs of international transactions; effect of global economy on UK economy   |
| 1.3 Socio cultural  | Demographic change affects demand for services; stakeholder expectations change   |
| 1.4 Technological   | Obsolescence of current systems; cost of procuring best technology available  |
| 1.5 Legal   | EU requirements   |
| 1.6 Environmental   | Buildings need to comply with changing standards; disposal of rubbish and surplus equipment needs to comply with changing standards   |
| <b>2. Operational (relating to existing operations – both current delivery and building and maintaining capacity and capability)</b>  |   |
| 2.1 Delivery  |   |
| 2.1.1 Service / product failure   | Fail to deliver the service to the user within agreed / set terms   |
| 2.1.2 Project delivery  | Fail to deliver on time / budget / specification  |
| 2.1.3 Capacity and capability   |   |
| 2.1.4 Resources   | Financial (insufficient funding, poor budget management, fraud)<br>HR (staff capacity / skills / recruitment and retention)<br>Information (adequacy for decision making; protection of privacy)<br>Physical assets (loss / damage / theft) |
| 2.1.5 Relationships   | Delivery partners (threats to commitment to relationship / clarity of roles)<br>Customers / Service users (satisfaction with delivery)<br>Accountability (particularly to Parliament)   |
| 2.1.6 Operations  | Overall capacity and capability to deliver  |
| 2.1.7 Reputation  | Confidence and trust which stakeholders have in the organisation  |
| 2.2 Risk management performance and capability  |   |
| 2.2.1 Governance  | Regularity and propriety / compliance with relevant requirements / ethical considerations   |
| 2.2.2 Scanning  | Failure to identify threats and opportunities   |
| 2.2.3 Resilience  | Capacity of systems / accommodation / IT to withstand adverse impacts and crises (including war and terrorist attack). Disaster recovery / contingency planning   |
| 2.2.4 Security  | Of physical assets and of information   |
| <b>3. Change (risks created by decisions to pursue new endeavours beyond current capability)</b>  |   |
| 3.1 PSA targets   | New PSA targets challenge the organisation’s capacity to deliver / ability to equip the organisation to deliver   |
| 3.2 Change programmes   | Programmes for organisational or cultural change threaten current capacity to deliver as well as providing opportunity to enhance capacity  |
| 3.3 New projects  | Making optimal investment decisions / prioritising between projects which are competing for resources   |
| 3.4 New policies  | Policy decisions create expectations where the organisation has uncertainty about delivery  |

## 5. ASSESSING RISKS



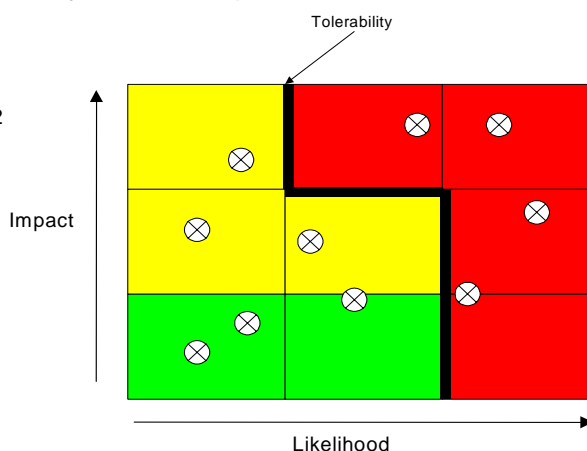
5.1 There are three important principles for assessing risk:

- be clear about the difference between, inherent and residual risk (see 2.2 and 2.4)
- ensure that there is a clear structure to the process so that both likelihood and impact are considered for each risk
- record the assessment of risk in a way which facilitates monitoring and the identification of risk priorities.

5.2 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 assessment is more of an art than a science. It will be necessary, however, to develop some framework for assessing risks. The assessment should draw as much as possible on unbiased independent evidence, consider the perspectives of the whole range of stakeholders affected by the risk, and avoid confusing objective assessment of the risk with judgement about the acceptability of the risk.

5.3 This assessment needs to be done in respect of both likelihood of the risk being realised, and of the impact if the risk is realised. A categorization of high / medium / low in respect of each may be sufficient, and should be the minimum level of categorisation – this results in a “3x3” risk matrix. A more detailed analytical scale may be appropriate, especially if clear quantitative evaluation can be applied to the particular risk - “5x5” matrices are often used, with impact on a scale of “insignificant / minor / moderate/ major/ catastrophic” and likelihood on a scale of “rare / unlikely / possible / likely / almost certain”. The organisation should reach a judgement about the level of analysis which it will find most helpful. When the assessment is then compared to the risk appetite (see 5.4 below), a “traffic light” approach is facilitated whereby those which are green do not require action, those which are amber should be monitored and managed down to green if possible, and those which are red require immediate action. It is not the absolute value of an assessed risk which is important; rather it is whether or not the residual risk is regarded as *tolerable*, or how far the exposure is away from tolerability which is important.

**Figure 5.1 Simple risk/tolerability matrix**  
 Adapted from SU report, *Risk [...]* Nov 02



5.4 At the organisational level risk appetite can become complicated (see section 11 for more detail), but at the level of a specific risk it is more likely that a level of exposure which is acceptable can be defined in terms of both tolerable impact if a risk is

realised, and tolerable frequency of impact of a realised risk. It is against this that the residual risk has to be compared to decide whether or not further action is required. Tolerability may be informed by the value of assets lost or wasted in the event of an adverse impact, stakeholder perception of an impact, the balance of the cost of control and the extent of exposure, and the balance of potential benefit to be gained or losses to be withstood.

- 5.5 Thinking about risk frequently focuses on residual risk (ie- the risk after control has been applied which, assuming control is effective, will be the actual exposure of the organisation - see 2.4). Residual risk, of course, will often have to be re-assessed if control is adjusted, and assessment of the expected residual risk is necessary for the evaluation of proposed control actions. However care should also be taken to capture information about the *inherent* risk. If this is not done the organisation will not know what its exposure will be if control should fail. Knowledge about the inherent risk also allows better consideration of whether there is over-control in place – if the inherent risk is within the risk appetite, resources may not need to be expended on controlling that risk. This need to have knowledge about both inherent and residual risk means that the assessment of risk is a stage in the risk management process which cannot be separated from addressing risk; the extent to which the risk needs to be addressed is informed by the inherent risk whereas the adequacy of the means chosen to address the risk can only be considered when the residual risk has been assessed.
- 5.6 Risk assessment should be documented in a way which records the stages of the process (an example is an Annex 1). Documenting risk assessment creates a *risk profile* for the organisation which:
- facilitates identification of risk priorities (in particular to identify the most significant risk issues with which senior management should concern themselves),
  - captures the reasons for decisions made about what is and is not tolerable exposure
  - facilitates recording of the way in which it is decided to address risk
  - allows all those concerned with risk management to see the overall risk profile and how their areas of particular responsibility fit into it
  - facilitates review and monitoring of risks.
- 5.7 Once risks have been assessed, the risk priorities for the organisation will emerge. The less acceptable the exposure in respect of a risk, the higher the priority which should be given to addressing it. The highest priority risks (the key risks) should be given regular attention at the highest level of the organisation, and should consequently be considered regularly by the Board. The specific risk priorities will change over time as specific risks are addressed and prioritisation consequently changes. The senior level attention given to risk management should be given to specific risk priorities, in respect of which specific action can be taken.

## 6. ADDRESSING RISKS



6.1 The purpose of addressing risks is to constrain them to an tolerable level (ie – within the risk appetite). Any action that is taken by the organisation to address a risk forms part of what is known as "internal control". There are five key aspects of addressing risk:

**TOLERATE:** The exposure may be tolerable without any further action being taken. Even if it is not tolerable, 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 to tolerate the existing level of risk. This option, of course, may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.

**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. This option is particularly good for mitigating financial risks or risks to assets. The transfer of risks may be considered to either reduce the exposure of the organisation or because another organisation (which may be another government organisation) is more capable of effectively managing the risk. It is important to note that some risks are not (fully) transferable – in particular it generally not possible to transfer reputational risk even if the delivery of a service is contracted out.

**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. This option can be particularly important in project management if it becomes clear that the projected cost / benefit relationship is in jeopardy.

**TREAT :** By far the greater number of risks will be addressed in this way. The purpose of treatment is that whilst continuing within the organisation with the activity giving rise to the risk, action (control) is taken constrain the risk to an acceptable level. Such controls can be further sub-divided according to their particular purpose (see 6.2 below)

**TAKE THE OPPORTUNITY**

This option is not an alternative to those above; rather it is an option which should be considered whenever tolerating, transferring or treating a risk. There are two aspects to this. The first is whether or not at the same time as mitigating threats, an opportunity arises to exploit positive impact. For example, if a large sum of capital funding is to be put at risk in a major project, are the relevant controls judged to be good enough to justify increasing the sum of money at stake to gain even greater advantages? The second is whether or not circumstances arise which, whilst not generating threats, offer positive opportunities. For example, a drop in the cost of goods or services frees up resources which can be re-deployed.

6.2 The option of “treat” in addressing risk can be further analysed into four different types of controls:

**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. Contingency planning is an important element of corrective control as it is the means by which organisations plan for business continuity / recovery after events which they could not control.

- 6.3 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 constrain risk rather than to eliminate it.

## 7. REVIEWING AND REPORTING RISKS

- 7.1 The risk which an organisation is managing has to be reviewed and reported on for two reasons:
- To monitor whether or not the risk profile is changing
  - To gain assurance that risk management is effective, and to identify when further action is necessary.
- 
- 7.2 Processes should be put in place to review whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks has changed, report significant changes which adjust risk priorities, and deliver assurance on the effectiveness of control. In addition, the overall process for risk management should be subjected to regular review to deliver assurance that it remains appropriate and effective. The review process should
- ensure that all aspects of risk management are reviewed at least once a year
  - make provision for alerting the appropriate level of management to new risks or to changes in already identified risks
- 7.3 A number of tools and techniques are available to help with achieving the review process
- Risk Self Assessment (RSA) is a technique which has already been referred to in the identification of risk (see 4.5). The RSA process also contributes to the review process. The results of RSA are reported into the process for maintaining the organisation-wide risk profile. (This process is also sometimes referred to as CRSA – “Control and Risk Self Assessment”)
  - “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. This process is compatible with CRSA; managers may use CRSA as a tool to inform the preparation of their Stewardship Report.
  - The Risk Management Assessment Framework, produced by the Treasury, provides a tool for evaluating the maturity of an organisation’s risk management. This tool is especially useful in preparing for the annual Statement on Internal Control which is a process orientated statement.
- 7.4 Every central government organisation is required to make provision for Internal Audit. Internal Audit’s work provides an important *independent* assurance about the adequacy of risk management. Internal audit may also 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 Internal Audit is neither a substitute for management ownership of risk nor a substitute for an embedded review system carried out by the various staff who have executive responsibility for the achievement of organisational objectives (see the “Government Internal Audit Standards”, HM Treasury, October 2001 and associated good practice guidance for more detail on internal audit issues).

7.5 Many organisations 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.

7.6 Except in rare circumstances, every government organisation will have an Audit Committee (established as a Committee of the Board, ideally with non-executive membership and Chaired by a non-executive) which will be charged with supporting the Accounting Officer in their responsibilities for issues of risk, control and governance and associated assurance (See the “Audit Committee Handbook, HM Treasury, October 2003 for more detail). The Audit Committee should be asked by the Accounting Officer / Board to:


- gain assurance that risk, and change in risk, is being monitored
- receive the various assurances which are available about risk management and consequently delivering an overall opinion about risk management
- comment on appropriateness of the risk management and assurance processes which are in place

However it should be noted that the Audit Committee should not itself own or manage risks and is, as with internal audit, not a substitute for the proper role of management in managing risk.

7.7 Some organisations may establish a Risk Committee. The Board need to decide what role it wants to assign to the Risk Committee. If the Risk Committee is established as a committee of the Board and is (largely) non executive (ie – a “Risk Assurance Committee”) it may undertake those functions outlined at 7.6 above which can appropriately be assigned to an Audit Committee; if, however, the Risk Committee is a forum for executive managers who have significant responsibility for the ownership and management of risk to meet together in order to share experience and co-ordinate their risk management actions (ie – a “Risk Management Committee” which discharges executive responsibility for ensuring that risk is effectively managed) the Audit Committee should retain the independent assurance role which is specified for it. The latter option does not preclude non-executive input to the considerations of the Risk Committee.

7.8 Annex 2 sets out the key process elements for both deriving and delivering overall assurance on risk management and provides a model for the assurance process.

## 8. COMMUNICATION AND LEARNING

- 8.1 Communication and learning is not a distinct stage in the management of risk; rather it is something which runs through the whole risk management process. There are a number of aspects of communication and learning which should be highlighted.
- 
- 8.2 The identification of new risks or changes in risk is itself dependant on communication. “Horizon scanning” (see 4.7 and Annex 2) in particular depends on maintaining a good network of communications with relevant contacts and sources of information to facilitate identification of changes which will affect the organisation’s risk profile. This can range from information on national security which could affect a government organisations strategic planning, through commercial intelligence about the viability of partner organisations or key contractors, to information about plans which one government organisation has which may affect demands made on another government organisation
- 8.3 Communication within the organisation about risk issues is important:
- It is important to ensure that everybody understands, in a way appropriate to their role, what the organisation’s risk strategy is, what the risk priorities are, and how their particular responsibilities in the organisation fit into that framework. If this is not achieved, appropriate and consistent embedding of risk management will not be achieved and risk priorities may not be consistently addressed
  - There is a need to ensure that transferable lessons are learned and communicated to those who can benefit from them. For example, if one part of the organisation encounters a new risk and devises an effective control to deal with it, that lesson should be communicated to all others who may also encounter that risk.
  - There is a need to ensure that each level of management, including the Board, receives appropriate and regular assurance about the management of risk within their span of control. They need to be provided with sufficient information to allow them to plan action in respect of risks where the residual risk is not acceptable, as well as assurance about risks which are deemed to be acceptably under control. As well as routine communication of such assurance there should be a mechanism for escalating important risk issues which suddenly develop or emerge.
- 8.4 Communication with partner organisations about risk issues is also important (see also Section 9 – The Extended Enterprise), especially if the organisation is dependent on the other organisation not just for a particular contract but for direct delivery of a service on behalf of the organisation. Misunderstanding of respective risk priorities can cause serious problems – in particular leading to inappropriate levels of control being applied to specific risks, and failure to gain assurance about whether or not a partner organisation has implemented

adequate risk management for itself can lead to dependence on a third party which may fail to deliver in an acceptable way.

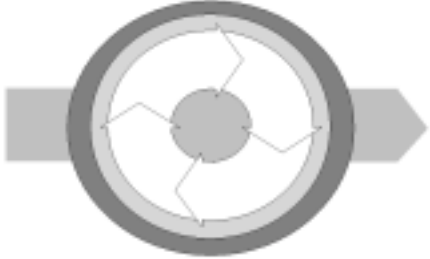
- 8.5 It is important to communicate with stakeholders about the way in which the organisation is managing risk to give them assurance that the organisation will deliver in the way which they expect, and to manage stakeholder expectation of what the organisation can actually deliver. This is especially important in relation to risks which affect the public and where the public depend on government to respond to the risk for them.

## 9. THE EXTENDED ENTERPRISE

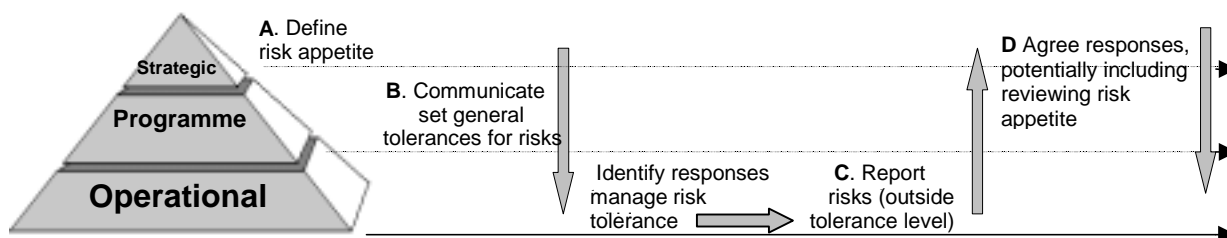
- 9.1 No organisation is entirely self-contained – it will have a number of interdependencies with other organisations. These inter-dependencies are sometimes called the “extended enterprise” and will impact on the organisation’s risk management, giving rise to certain additional risks which need to be managed. These considerations should include the impact of the organisation’s actions on other organisations. This section highlights some potential extended enterprise relationships and the risk management implications which might arise.
- 9.2 Many organisations will have inter-dependencies with other Government organisations with which they do not have a direct control relationship – the delivery of their objectives will depend upon / impact upon the delivery of the other organisations objectives. In these circumstances what one organisation does will have a direct impact on the risks which another organisation faces, and effective liaison between the two organisations is essential to facilitate an agreed risk management approach which will allow both to achieve their objectives.
- 9.3 Many government organisations will have a relationship with bodies which they either “parent” or which have a “parent” role over them. In particular many policy departments are dependant on Executive Agencies or Non-Departmental Public Bodies (NDPBs) for delivery of their policy, and many Executive Agencies and NDPBs are constrained in policy by their parent department. In these circumstances the risk priorities of a parent department will impact on the priorities of the organisations which they sponsor, and the sponsored organisations’ experience of managing risk in delivery of the policy needs to be considered by the parent organisation in the further development of policy. Regular and open discussion of risk issues between parent organisations and sponsored organisations is critical to the overall effective delivery of public service.
- 9.4 Probably all government organisations will have dependencies on contractors, although the extent of these dependencies will vary. These relationships may range from straightforward supply of goods which the organisation requires in order to function, through to delivery of major services to, or on behalf of, the organisation. This could include Public Private Partnerships or contracted out services such as delivery of the IT infrastructure for the organisation. A particular potential problem here is when the organisation has a high dependency on a contractor, but the organisation is only a minor client for the contractor (for example, a small NDPB purchasing bespoke software from a major IT consulting firm). It is important that organisations consider each of their relationships with contractors and ensure that appropriate communication and understanding about respective risk priorities is achieved.



## 10. RISK ENVIRONMENT AND CONTEXT

- 10.1 Beyond the boundary of the “extended enterprise”, other factors contribute to the environment in which risk has to be managed. These factors (generally those in the “external” risk grouping in the table in Section 4) may either generate risks which cannot be directly controlled, or they may constrain the way in which the organisation is permitted to take or address risk. Often the only response which an organisation can make in relation to the risk environment is to prepare contingency plans. For example, most government organisations with central London headquarters cannot directly control the risks arising from international terrorism, but they can make contingency plans for how to ensure business continuity in the event of a major terrorist attack. (see [www.ukresilience.info/lead.htm](http://www.ukresilience.info/lead.htm) for more information) It is important that an organisation should consider its wider risk environment and identify the way in which it impacts on its risk management strategy.
- 
- 10.2 In particular, laws and regulations, can have an effect on the risk environment. It is important for an organisation to identify the ways in which laws and regulations make demands on it, either by requiring the organisation to do certain things or by constraining the actions which the organisation is permitted to take. For example, the way in which an organisation handles the risk of staff performing inadequately is constrained by employment legislation.
- 10.3 The economy, both domestically and internationally, is another important element of the risk environment. Whilst for most organisations the general economy is a given, it does affect the markets in which they have to function in obtaining or providing of goods and services; in particular the economy can have an effect on the ability of an organisation to attract and retain staff with the skills which the organisation needs.
- 10.4 A particular aspect of the risk environment which is important for government organisations is Government itself. In principle, government organisations exist to deliver the policies which the Government and its Ministers have decided upon. There is a particular strand of risk management which is important in providing Ministers with risk based policy advice. Nevertheless, officials in government organisations may be constrained in the risks which they do or do not take by policy decisions.
- 10.5 Every organisation is also constrained by stakeholder expectation. Risk management actions, which appear good value and effective in the abstract, may not be acceptable to stakeholders. For government organisations this is especially important in respect of relationships with the public (see 8.5); actions that would be effective at dealing with a specific risk may have other effects that the public are unwilling to accept.

# 11. RISK APPETITE



## 1) Corporate Risk Appetite

Corporate risk appetite is the overall amount of risk judged appropriate for an organisation to tolerate, agreed at board level (letter A above). This may not be just one statement: OGC, for example, look at 5 key risk areas (policy/guidance risk; people and internal systems risk; propriety, regularity, finance and accountability risk; reputation risk; external risk) and make a statement on risk appetite for each (see OGC’s example below).

The Board and senior managers should judge the tolerable range of exposure for the organisation and identify general boundaries for unacceptable risk (or at least for risks that should always be referred to / escalated up to the Board for discussion and decision when they arise). In doing this the Board may want to take Ministerial views on risk-taking into account.

## 2) Delegated Risk Appetite

The agreed corporate risk appetite can then be used as a starting point for cascading levels of tolerance down the organisation, agreeing risk appetite in different levels of the organisation (letter B above). This then means that different levels of the organisation are clear on the boundaries in which they are operating, and feel confident about the amount of risk they are exposed to.

## 3) Project Risk Appetite

Projects that fall outside of day-to-day business of an organisation might need their own statement of risk appetite. Different types of projects might also require different levels of risk appetite, for example an organisation may be prepared to accept a higher level of risk for a project that would bring substantial reward.

3 different types of project could be:

- a) Speculative (akin to venture capitalism in the corporate sector): with high risks but potentially innovative rewards, e.g. Defra’s Futures programme area; Invest to Save Budget projects; Pilot projects. It may be that the bulk of these projects are unsuccessful but important lessons are learnt.

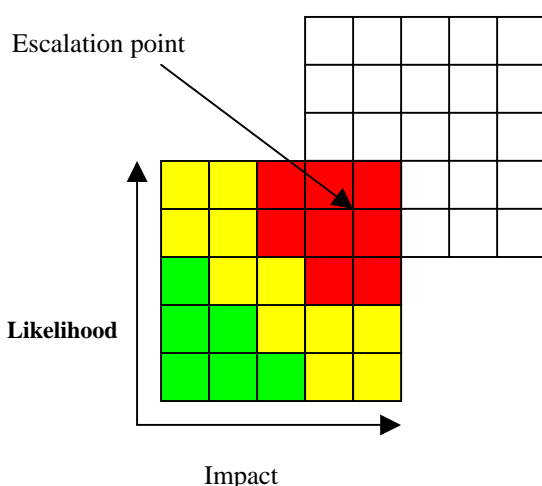
- b) Standard development projects: for example IT, procurement etc., and those covered by OGC’s Centres of Excellence programme, which aims to improve the success rate of these projects from 35% to 70% by end 2005.
- c) ‘Mission critical’ projects: where organisations need to be sure of success.

The level of risk appetite will obviously vary, with a project of type a prepared to take on higher levels of risk than type c.

## USING RISK APPETITE

### 1) Escalation

When different levels of the organisation have a hierarchy of tolerance levels, it is possible to set ‘trigger points’ where risks can be escalated to the next level as they approach or exceed their agreed risk appetite levels (letter C above). For example, a definition of ‘high’ risk at one level in the organisation could mean that the risk needs to be escalated to the next level.



The next level up in the hierarchy would then take appropriate action, which may mean managing the risk directly, or could mean adjusting the level of risk that they are happy for the level below to manage (letter D above).

### 2) Resource allocation

Once the risk appetite level is set, it is possible to review if resources are targeted appropriately. If a risk does not correspond to the agreed risk appetite, resources could be focused on bringing it to within the tolerance level. Risks which are already within the agreed tolerance level could be reviewed to see if resources could be moved to more risky areas without negative effects. Customs, Inland Revenue, the Police and Fire Service all use risk-based resource allocations to prioritise allocation of resources.

### 3) Project initiation

When taking the decision whether to initiate a new project, and when undertaking subsequent OGC Gateway reviews, risk appetite can be used as a guide on whether to proceed with the project and also to help identify and manage risks which may impede the success of the project.

## Annex 1

### Example of documenting risk assessment

| OBJECTIVE – To travel from A to B in time for an important meeting |                     |            |  |                     |            |  |             |             |
|--|---------------------|------------|--|---------------------|------------|--|-------------|-------------|
| RISK   | Inherent assessment |            | CONTROLS IN PLACE  | Residual assessment |            | ACTION PLANNED   | TARGET DATE | OWNER       |
|  | Impact              | Likelihood |  | Impact              | Likelihood |  |             |             |
| Missing a train makes me late for the important meeting            | High                | High       | Catch train one earlier than I actually need                                 | High                | Low        | No further action planned  |             | M. Y. Self  |
| Severe weather prevents the train from running                     | High                | Low        | Cannot control   | High                | Low        | Telephone conferencing facility to be installed as a contingency | August      | A. N. Other |
| Engineering works make the train late                              | High                | Medium     | Check for engineering works and arrange flexibility with people I am meeting | Medium              | Low        | No further action planned  |             | M. Y. Self  |

## Annex 2

# Overall Assurance on Risk Management

### Principles of Assurance

#### 1. Planning to gain assurance:

- 1.1 Assurance strategy – overall assurance will only be gained if there is a strategy for obtaining it. The Assurance Strategy should be approved by the Board and Audit Committee
- 1.2 Assurance process – the processes for obtaining assurance should be embedded into existing processes

#### 2. Making explicit the scope of the assurance boundaries:

In order to arrive at an overall opinion the scope of the processes required for obtaining assurance need to encompass the whole of the organisation's risk management lifecycle. This does not mean that every risk and every control has to be reviewed in order to obtain assurance. However, the review, which takes place, will need to provide:

- 2.1 Assurance on the Risk Management Strategy - Ascertain the extent to which all line managers review the risks / controls within the ambit of their responsibility
- 2.2 Assurance on management of risks/controls themselves - encompass all the key risks and encompass enough of the other risks to support confidence in the overall opinion reached
- 2.3 Assurance on the adequacy of the review/assurance process - quality assured to engender confidence in the review process

#### 3. Evidence:

The evidence supporting assurance should be sufficient in scope (2.2) and weight (4.2) to support the conclusion and be:

- relevant
- reliable
- understandable
- free from material misstatement
- neutral/free from bias
- such that another person would reasonably come to the same conclusion

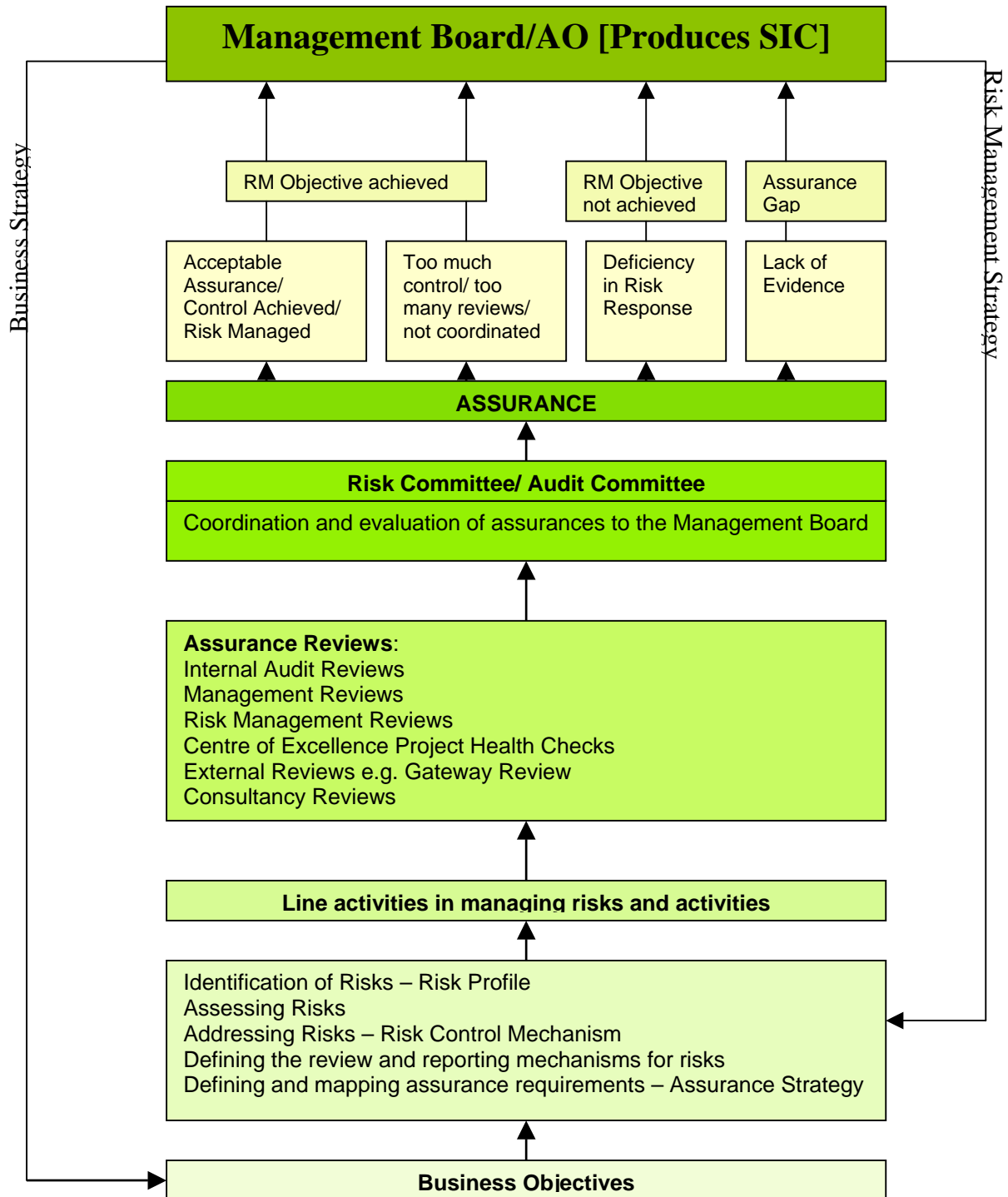
#### 4. Evaluation:

##### 4.1 The objective is to:

- evaluate the adequacy of the risk management policy and strategy to achieve its objectives,
- evaluate the adequacy of the risk management processes designed to constrain residual risk to the risk appetite

- identify limitations in the evidence provided or in the depth or scope of the reviews undertaken
  - identify gaps in control and/or over control, and provide the opportunity for continuous improvement, and
  - support preparation of the SIC
- 4.2 In evaluating evidence to arrive at an overall judgment or opinion all of the evidence criteria at 3 need to be considered. However it is important to recognise that:
- Not all evidence is of the same weight in deriving assurance. Evidence should be weighted:
    - ◇ According to its independence – the more independent the evidence, the more reliance can be placed on it. However circumstances may exist that could affect the reliability of the information obtained, e.g. for independent external evidence to be reliable the source of the evidence must be also knowledgeable.
    - ◇ According to its relevance – in determining the overall assurance there is a need to ensure that the evidence relates to those elements of the risk management lifecycle considered to be significant - evidence relevant to the more significant risks is consequently of greater relevance to the overall assurance
  - Evidence may be flawed in terms of both quantity and quality where the evidence criteria are not met, leading to limitations in the assurance that can be provided. For example, merely obtaining more evidence will not compensate where the quality of evidence is low or where the source of evidence is not reliable.
5. Reviewing and Reporting:
- 5.1 Assurances are reported from many different sources within an organisation: from external sources, from suppliers and contractor, from third parties, from management and practitioner review internal to the organisation and from internal independent or neutral sources etc. The Assurance Strategy needs to define stages where assurances will be evaluated and opinions reported through the various layers of management to the Board.
- 5.2 Assurance opinions need to be reported clearly, and worded so as to clearly communicate the scope and criteria used in arriving at those conclusions.

The Assurance Model



## Annex 3

### Summary of Horizon Scanning Issues

*Provided by the Civil Contingencies Secretariat of Cabinet Office*

- **Periodicity / Regularity:** horizon scanning may be continuous (in an organisation like the Civil Contingencies Secretariat (CCS) which continuously searches for potential future disruptive challenges) or periodic (e.g. weekly or annually).
- **Timescale:** Policy makers could well be interested in developments over the next twenty-five years whilst horizon scanning that supports operational decision making may be restricted to a six month timeframe.
- **Scope:** Some organisations may be fairly insular in their risk identification processes if they perceive that the major element of risk arises from within the organisation; others may need to consider a much wider scope if they consider that they may face risks from a wider environment. Depending on the nature of the organisation's business this element of risk identification may range from almost exclusively internal activity to activity that depends on international networks of technical information.
- **Opportunity/threat:** Some horizon scanning is concerned mainly with spotting potential problems, but it can equally be used to scan for opportunities ("positive risks"), and many problems may be translatable into opportunities if spotted early enough.
- **Rigour / technicality:** Horizon scanning varies in the extent to which it is structured and supported by technology. Some organisations use sophisticated assessment schemes and information search technologies; other organisations will rely almost entirely on informal networks of contacts and good judgment

[see [www.ukresilience.info/home.htm](http://www.ukresilience.info/home.htm) for more information]

## Annex 4

### Glossary of key terms

|                                       |  |
|---------------------------------------|--|
| <b>Assurance –</b>                    | an evaluated opinion, based on evidence gained from review, on the organisation's governance, risk management and internal control framework.  |
| <b>Audit Committee –</b>              | a Committee appointed to support the Accounting Officer (in NDPBs a Committee of the board to support the Board) in monitoring the corporate governance and control systems in the organisation. |
| <b>Exposure –</b>                     | the consequences, as a combination of impact and likelihood, which may be experienced by the organisation if a specific risk is realised.  |
| <b>Inherent Risk –</b>                | the exposure arising from a specific risk before any action has been taken to manage it.   |
| <b>Residual risk –</b>                | the exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective.   |
| <b>Risk –</b>                         | uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance.                  |
| <b>Risk appetite –</b>                | the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time.  |
| <b>Risk assessment –</b>              | the evaluation of risk with regard to the impact if the risk is realised and the likelihood of the risk being realised.  |
| <b>Risk Assurance –<br/>Committee</b> | a Committee established to undertake the role which the Audit Committee should otherwise undertake in respect of assurance on risk management.   |
| <b>Risk management –</b>              | all the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.               |
| <b>Risk Management –</b>              | a Committee established with executive authority to  |

|                           |   |
|---------------------------|---|
| <b>Committee</b>          | take action to manage the risks which face the organisation.  |
| <b>Risk strategy –</b>    | the overall organisational approach to risk management as defined by the Accounting Officer and / or Board. This should be documented and easily available throughout the organisation                  |
| <b>Risk profile –</b>     | the documented and prioritised overall assessment of the range of specific risks faced by the organisation  |
| <b>Internal control –</b> | any action, originating within the organisation, taken to manage risk. These actions may be taken to manage either the impact if the risk is realised, or the frequency of the realisation of the risk. |