Management Board

Corporate Risk Management: March 2008

Paper by the Head of the Office of the Chief Executive

Purpose of this paper

1. This paper is the quarterly update to the Management Board on risk management. It proposes a way forward for the risk management process in light of the recent changes to the organisational structure.

Decisions

2. The Board is asked to:

i. Approve:
the House of Commons: Risk Management policy (Annex A);
the House of Commons Risk Management Principles and Concepts Manual (Annex B); and
ii. Note the work in progress on producing a House of Commons: Risk Guidance Manual and approve principle (para 11);
iii. Note the work in progress in re-aligning Departmental risk registers (paras 12-14);
iv. Note the proposed risk escalation process and risk workshops for risk owners across the House (para 15);
v. Note the programme of corporate risk reviews for the Board (paras 16-17);
vi. Approve resources for a "risk healthcheck" (para 20);
vii. Nominate a senior manager to present a risk issue to the April Audit committee meeting (para 21).

RISK MANAGEMENT: BACKGROUND

3. Since the risk management process moved into the OCE in January 2008, much work has taken place on reviewing how risk is currently managed within the House, how it links with audit and business continuity planning and how we can put in place a more robust risk management framework which assists the Board in the achievement of its objectives and meets the levels of assurance required by the auditors and the Statement of Internal Control.

Impact of Organisational Structure

4. The recent structural changes have reduced the number of House departments from six to four functionally based departments. The departments are headed by Director Generals (DGs) who sit on the Management Board (MB). As members of the MB the DGs represent their function from a corporate rather than a departmental perspective and have joint and several responsibility. These changes together with the creation

of a joint House department for information and communication technology mean that the previous arrangements for corporate risk management need to be adapted to fit the new environment.

PwC Audit

5. There have been four annual reviews of risk management and all have concluded that there is still more to be done before any meaningful assurance could be given. The last review of risk, conducted by PwC in November 2007, concluded that only limited assurance could be given on the adequacy of the current arrangements, which was disappointing, considering the level of energy directed towards risk management over the last year.

Key weaknesses identified by PwC

6. The main areas that require attention are:

   i. The corporate risks need to be more closely linked to business objectives.
   ii. Risk managers need to have an increased part to play when departmental risks are reviewed.
   iii. Risk management should be embedded in the management processes of the House.
   iv. Departmental risk registers are poor; there needs to be consistency between and within departments.
   v. The corporate risk register is complex and difficult to interpret quickly.
   vi. Maintaining the risk registers appears to take priority over managing the risks.
   vii. The escalation of risks through the organisation is weak.

RISK MANAGEMENT: WAY FORWARD

Step One: How do we improve?

7. The aim is to build on the present risk management process. In this way we would hope to create a system that is more robust and effective. To do so we need to ensure that:

   i. Members of the Management Board are engaged in and champion risk management across the House;
   ii. Departmental risk champions are identified, to facilitate and assist risk owners within their own departments, this will need to be recognised as a significant time commitment in their job descriptions;
   iii. The risk management system (RMS) is simple and easy to understand and capable of being used by staff at all levels;
   iv. The risk registers are easy to maintain;
   v. The RMS is capable of dealing with all risks from corporate and strategic risks to low level operational risks;
   vi. There is consistency across and within departments;

vii. The focus is also on bottom-up risk identification, not just top down; and

viii. Risk reporting includes bottom up escalation i.e. up the departmental tree to departmental registers and to Board level.

Step Two: What is needed?

A) House of Commons Risk Management Documentation

8. The House has had a risk management policy statement and implementation strategy in place since 2001, which follows best practice as recommended by the Treasury (Management of Risk – A Strategic Overview H M Treasury Jan 2004). However, one of the main criticisms, of the 2007 PwC audit, was the lack of up to date documentation on risk management within the House, the Board is therefore asked to approve the following two risk management documents:

1. House of Commons Risk Management Policy (Appendix A)

9. This document sets out the proposed House of Commons Risk Management Policy and Strategy. It acts as the foundation for the House's risk management process, and provides a basis for all supporting documentation. It continues to follow best practice as recommended by the Treasury.

2. House of Commons: Risk Management Principles and Concepts (Appendix B)

10. This document sets out the principles and concepts of risk management and is based upon the Treasury's Orange Book 2004 (Management of Risk – A Strategic Overview).

11. A third document is also planned, the House of Commons: Risk Management Guidance Notes, which is aimed at managers and staff who are responsible for managing risks on a day to day basis. It will provide an easy to follow, step-by-step guide to how the risk management process works.

B) Improvement in Department Risk Registers

12. The November 2007 PwC audit found that the overall quality of the risk registers were still poor with inconsistencies between departments. Since then, a review of departmental risk registers took place in January 2008, by the Director of FMD, Chris Ridley, and the Risk Management Facilitator (RMF), [s.40], who found that although departments have continued to develop their risk registers in line with board recommendations, some departments had progressed better then others.

13. BPG agreed that Departments should take forward the following issues when realigning their 2008/09 risk registers to reflect the new departmental structures:

i. Ensure that new departmental risk registers are succinct and clear. (A format for a standard summary risk register was agreed based upon a risk heat map).
ii. Better cross-referencing between corporate and departmental risks with the identification of local departmental risks as well as corporate related risks. For example, local skill or system risks might prevent a department from delivering its objectives but do not directly link back to the more strategic corporate risks. This could be described as 'bottom up' as well as 'top down' risk management.
iii. Improve the quality of information provided as evidence in support of mitigating actions i.e. more specific and measurable.
iv. The identification of any transitional risks associated with the Tebbit change programme in addition to the business as usual risks normally captured.

14. This work has now commenced. Departmental risk registers will be re-aligned to reflect the new unified structure, with a summary being included within 2008/09 Departmental Business Plans (meeting the recommendation by the Business Continuity Policy Steering Group that risk registers be revised to reflect the new structure). The intention is to review those new registers and those registers covering the period 1 January to 31 March (which will support the Statement of Internal Control in the Resource Accounts) in April 2008 with feedback to the Board for the May 2008 board meeting.

C) A System for the Escalation of Risks

15. Another key criticism from PwC was the lack of a risk escalation process within the House i.e. between departmental and corporate risk registers. To "kick start" this process, OCE intend to hold risk workshops in April 2008 with key risk owners (from departments and major projects) who will be asked to prioritise and rank their risks. The top two/three risks will then be mapped onto a risk heat map and presented to the MB who will be able to decide (after consideration of the consequences or impact of those key risks) whether any should be incorporated into the corporate risk register. This should go some way towards ensuring that the corporate risk register does not remain static. The intention is to put in place a system for presentation to the Board at the May 2008 board meeting.

D) Regular Corporate Risk Review/Annual Corporate Risk Review

16. In the meantime, the regular corporate risk reviews (i.e. the meetings with the relevant Director General and RMF) will commence soon to ensure that we do not lose sight of business as usual. For information, it was agreed in November 2007, that the corporate risks be allocated by functional area to one Director General for overall responsibility as follows:

1	Disruption to the work of the House or other services as a result of terrorist attack	Douglas Miller
2	Disruption to the work of the House or other services as a result of an unplanned event (e.g. fire, flood, public disorder, health epidemic, etc).	John Borley
3	Disruption to the work of the House or other services as a result of a major IT breakdown or the failure to develop an IT infrastructure that is robust.	John Pullinger Joan Miller
4	The rate and nature of organisational and cultural change leads to a deterioration in services.	Andrew Walker
5	The House administration suffers loss of reputation and/or financial loss through failing to comply with legal requirements, audit and accounting requirements, and/or through demonstrably poor value for money in the delivery of its services.	Andrew Walker
6	A major project or change programme fails to deliver the expected benefits in line with the planned investment agreed in the business case.	John Borley
7	The House suffers loss or disruption to services through a failing in contract procurement or supplier management.	Andrew Walker
8	The House administration is unable to carry forward a consistent strategy because of the conflicting demands of key stakeholders in the House and dependencies on the House of Lords.	Douglas Miller

17. The Board, in previous years, reviewed its top corporate risks just before the summer recess (the aim being to ensure the risks remain relevant in light of any changes in corporate strategy). For this year, the intention is, again, to hold a risk review but towards the end of the summer recess, to allow time for the departmental risk escalation process to embed.

E) Training and Communication of Risk

18. It is essential to the objective of embedding risk management into the House's processes that the Board agrees to instigate a training and communication framework for risk. If the Management Board approves the attached policy, principles and concepts, the next step will be to work with Departments to ensure that they understand how they should be applied. The aim will be:

    i. to hold risk presentations at team meetings and management away days,
    ii. to include risk management sessions within management training courses; and
    iii. to undertake "risk roadshows" to promote risk management across the House.

OTHER RISK ISSUES

Resourcing of Risk

19. As a result of the Board's agreement to additional internal resources to support the risk management process, a part-time Band B1 has been assisting the Risk Management facilitator since the beginning of January.

20. It is proposed that the Board now "buy in" some external risk expertise to instigate a "health check" on our risk management system. This might be [s.40], who recently facilitated a training session with the Audit Committee. This will not only provide assurance to the Board that we are on track to embed risk management across the House but also ensure we are keeping in line with best practice. We envisage a cost of £10,000 - £15,000 based upon 5 days' consultancy work.

Audit Committee

21. One of the outcomes from the Audit Committee meeting in January 2008 was a request by the Audit Committee (as part of its aim to take on a role of constructive engagement with risk management within the House) to talk regularly to senior managers across the House directly responsible for managing risk. The Board is asked to nominate a senior risk owner to attend the next committee meeting in April and consider candidates for subsequent meetings.

Risk Timetable

22. It is one of the OCE's key targets to secure improved assurance when the House's risk management policy and procedures are next reviewed. The next review is planned for early to spring 2009. By spring 2009 it is our intention to ensure the new risk management system in place and working effectively. However, because the new system would not have been in operation for very long it may be difficult to achieve a high assurance opinion at that stage. We therefore intend to use the review to confirm that what is in place, and any further developments envisaged at that time are sound and would secure a high level of assurance if they were operated as intended.

23. The proposed timetable for this year is as follows:

Date	Action	Owner
April 2008	Review of Departmental risk registers Departmental/Major Project Risk workshops to establish escalation process "Risk Healthcheck" on risk process	RMF Risk Management Facilitator (RMF) /OCE OCE
May 2008	Feedback to Board on review of departmental risk registers Feedback to Board	RMF

	on key risks identified at risk workshops	
April –June 2008	Regular evaluation and review of current corporate risks.	MB RMF
Sept 2008	Annual Corporate Risk Review “Risk Roadshow”	MB RMF OCE

Philippa Helme
Head of the Office of the Chief Executive

March 2008

Appendix A

House of Commons Risk Management Policy and Strategy
Introduction

This document sets out The House of Commons policy and strategy for the identification and management of risk, including the roles and responsibilities of all managers and staff across the organisation.

Guidance and briefing on the day-to-day assessment and management of risk are set out in the House of Commons Risk Management: Guidance notes.

The policy on management of risk

The identification and management of risks affecting the House's ability to achieve its objectives are key responsibilities of all managers and staff of the House. The effective management of risk is an important means by which the House achieves its goals. To that end the House's policy is to:

a. manage risk actively across the full breadth of operations within the House.
b. devolve responsibility for risk ownership and risk management to the most appropriate local level within the House, but complementing this with oversight and monitoring mechanisms
c. integrate local risk management with local business planning (the business planning process is used to set objectives, agree action plan and allocate resources)
d. develop understanding of a risk–aware approach to working
e. provide and maintain guidance on the techniques of risk assessment and risk management
f. monitor and report regularly and frequently on the management of risk; and
g. keep policy and practice under review.

The key principles

The following key principles underlie the House's approach to risk management:

- This policy forms part of the House's corporate governance and internal control and assurance arrangements.
- Risk management is one of the key tools to ensure the achievement of the House's business objectives set out in its strategic Corporate and annual departmental business plans, and as such is an integral part of planning and monitoring.
- Risk management is a process for defining, analysing, controlling and managing risk.
- The Management Board is ultimately responsible for the internal control arrangements, including risk management.

The House defines risk as:

'The threat that an action or event will adversely affect the House's ability to achieve its current and future objectives.'

In its management of risk, the House makes a distinction between strategic (corporate) risk and operational risk. This distinction is reflected in the respective roles of the Management Board, second tier management groups (HRG, BPG) and Departments of the House.

- Operational risks are primarily to do with the day-to-day conduct of the House's business or the management of the House as an organisation – governance, staffing, resourcing, procedural and administrative systems. The management of operational risk is an integral part of business planning, management and monitoring, that has been delegated to Departments and, where appropriate, the second tier management groups.
- Strategic risks are different. They are invariably less to do with the day-to-day conduct of the business of the House and are more to do with the nature and purposes of the organisation, its ability to achieve its mission, the environment it operates in, the needs of Members of Parliament and other stakeholders and the reputation of the House. Strategic risks are identified and managed by the Management Board through its own annual assessment of risks. Key strategies for managing strategic risks include adaptability and responsiveness, working in partnership with stakeholders to understand and meet their needs, developing expertise so that the organisation can respond to change as circumstances alter.

Risk management strategy: roles and responsibilities
Role of the Management Board

The Management Board has ultimate responsibility for the management of risks. It monitors the approach to the management of risk, and its effectiveness in managing risk and the implementation of this risk management policy and reporting requirements. It considers the risks facing the House at a strategic level. Its role includes:

- instilling a culture of risk management:
- satisfying itself that risks are managed appropriately:
- identifying emerging strategic risks;
- approving the overall risk management arrangements;
- monitoring the management of significant risks;
- satisfying itself that the less significant risks are being actively managed, and that the appropriate controls in place are working effectively;
- annually reviewing the approach to risk management and approving key changes or improvements to processes and procedures.

Role of the Audit Committee

As part of the Audit Committee's role to advise the Accounting Officer on the effectiveness of the House's internal control arrangements, it will:

a. annually review the House's approach to risk management and overall risk management arrangements
b. advise the Accounting Officer on the implications of internal audit reports and the recommendations made by the external auditors.

Role of the Office of the Chief Executive

The Risk Facilitation function resides in the Office of the Chief Executive (OCE), which supports the Clerk in his role as Chief Executive of the House of Commons. Under the direction of the Head of OCE, the House's risk facilitation team is responsible for:

- maintaining the House Risk Management policy, strategy and guidelines;
- facilitating the Management Board in its annual identification and assessment of the strategic risks faced by the House and the updating of the corporate risk register;
- overseeing the assessment of operational risks (at departmental level) and the preparation of risk registers; and
- preparation of reports to the Audit Committee and the Management Board.

Role of the Director Generals

Their role is to identify, assess, manage, monitor and report on the management of operational risks at the Group level. Specifically, as part of the development of local operating plans. Director Generals are responsible for:

a. devising an appropriate local mechanism for identifying, assessing, managing, monitoring and reporting on risk which reflects the House's risk management policy;
b. implementing policies on risk management and internal control arrangements at the departmental level;
c. as part of the annual business planning exercise describing risks identified and how they are being managed in accordance with the House's risk management guidelines;
d. identifying, assessing and developing a strategy to manage risks for the objectives set out in the departmental business plans;
e. monitoring the management of the risks for which they are responsible; and
f. providing adequate information to the Management Board, on the status and management of risks.

Role of staff

All employees of the House are expected:

- to be familiar with the House's policy on and approach to risk management;
- to take a risk management approach to their work;
- to take responsibility for the risks they 'own;'
- to highlight ways in which the business objectives may be at risk and could be managed better; and
- to consider how the House might reduce its exposure to risk.

Risk management as part of the system of internal control

The system of internal control incorporates risk management. Together, a number of elements facilitate the effective management of risks. These elements in the House include:

- risk management policies and procedures
- Comprehensive reporting to monitor key risks and their controls
- Business Planning Process used to set objectives, agree action plans and allocate resources
- Corporate risk register
- Departmental risk register
- Audit Committee
- Internal Audit
- External Audit
- Other sources of assurance within the House, eg: Health and Safety, specialist consultants etc; will increase the reliability of the system of internal control.

Appendix B

HOUSE OF COMMONS

MANAGEMENT OF RISK

PRINCIPLES AND CONCEPTS

HOUSE OF COMMONS
March 2008

CONTENTS

PURPOSE

1.1 This documents sets out the risk management principles and concepts for the House of Commons and describes the general principles and corporate definitions of risk and risk management which have been adopted by the House.

1.2 The Clerk, as Accounting Officer and Chief Executive, and the House of Commons Management Board (MB), of which the Clerk is Chairman collectively own and support this policy and guidance document. Its intention is to ensure consistency of approach across the House of Commons.

2. OVERVIEW

Background

The House has had a risk management policy statement and implementation strategy in place since 2001, which follows best practice as recommended by the Treasury (Management of Risk – A Strategic Overview H M Treasury Jan 2004). This has since been revised and adopted by the Management Board in March 2008. A copy of which is in Annex 1.

Risk Management is an integral part of the process of signing the annual Statement of Internal Control, signed by the Accounting Officer – The Clerk of the House and the letters of assurance regarding the management of business risks required in support of that statement.

What is risk management?

2.2 The identification and management of risks affecting the House's ability to achieve its objectives are key responsibilities of all managers and staff of the House. 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 happen.

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.

2.4 The response to risk is called "internal control" (mitigations) and is initiated from within the House of Commons. It may involve one or more of the following:

- tolerate the risk, i.e. accept the risk without doing anything.
- transfer the risk, e.g. outsourcing PWC contract.
- terminate the activity giving rise to the risk, i.e. stop doing it.
- 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, i.e. take mitigation/risk prevention.

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 (see section 5).

2.5 None of this takes place in a vacuum. The House of Commons Administration operates within an environment which both influences the risks faced and provides a context within which risk has to be managed. Further, the House has partners on which it depends in the delivery of its

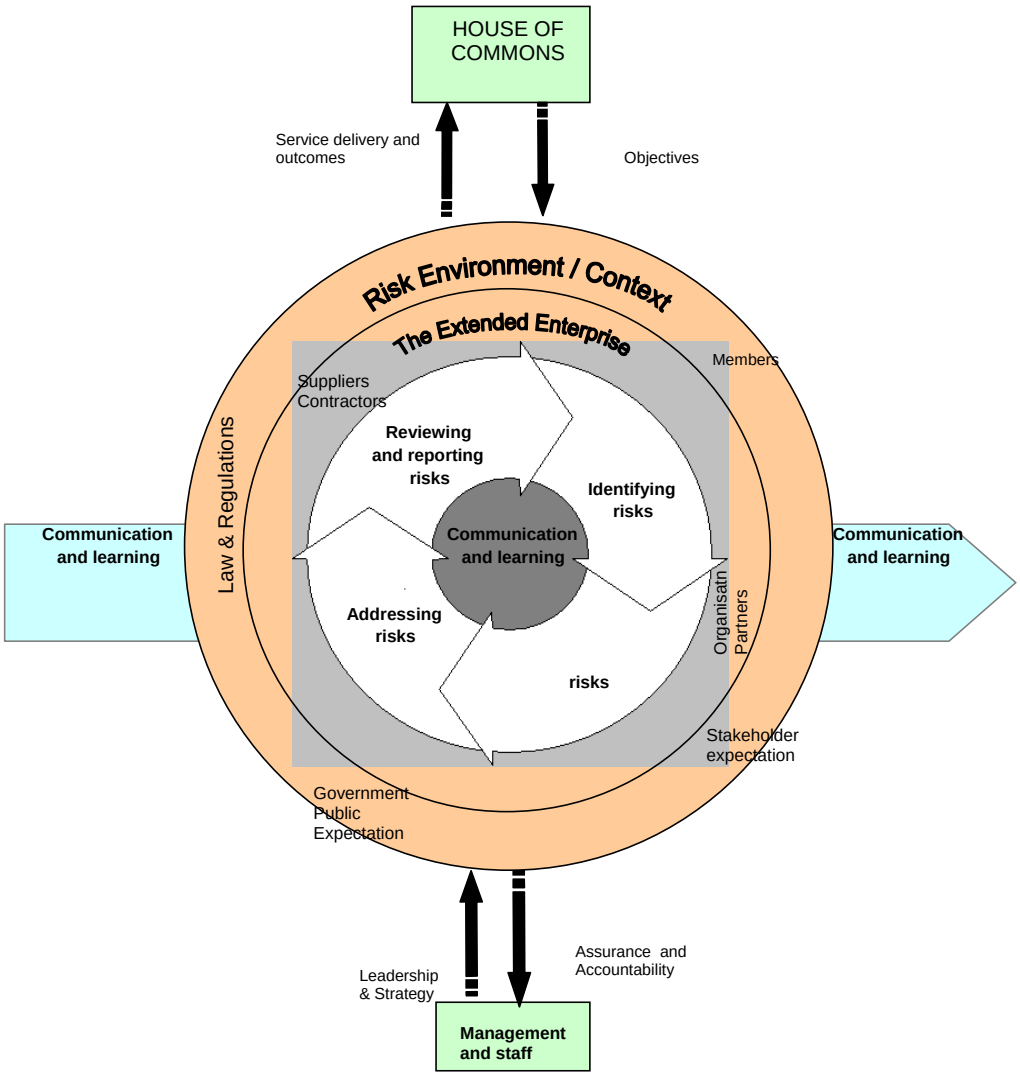
objectives whether they be simply suppliers of goods which the House requires or direct partners in the delivery of objectives.

2.6 All of this means that the House of Commons Administration, which wants to maximize its success in delivering its objectives, needs to have a risk management strategy, led from the very top of the House, which is then implemented by managers at every level of the House in the particular activities which they manage, and embedded in the normal working routines and activities of the House. The management of risk at strategic, programme and operational levels needs to be integrated so that the levels of activity support each other.

2.7 Managers at every level therefore need to be equipped with appropriate skills which will allow them to manage risk effectively and the House as a whole needs a means of being assured that risk management is being implemented in an appropriate way at every level.

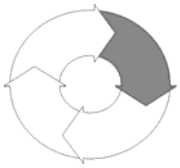
2.8 This principles and concept aims to provide an introduction to the range of considerations which apply in risk management, all of which can be applied at various levels ranging from the development of a strategic, House-wide risk policy through to management of a particular project or operation.

THE RISK MANAGEMENT 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, 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.
- 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.

3. IDENTIFYING RISKS



3.1 In order to manage risk, the House needs to know what risks it faces, and to evaluate them. Identifying risks is the first step in building the House's risk profile.

3.2 The identification of risk can be separated into two distinct phases. There is:

- initial risk identification (for a new project or activity within the House), 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 have ceased to be relevant to the House.

3.3 In either case risks should be related to objectives. Risks can be assessed and prioritised in relation to objectives. When a risk is identified it may be relevant to more than one of the House'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.

Objective – 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	**X** this is simply the converse of the objective
Being late and missing the meeting	**X** 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	**X** this does not impact on achievement of the objective
Missing the train causes me to be late and miss the meeting	✔ 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	✔ This is a risk which I cannot control, but against which I can make a contingency plan

3.4 Typically a department within the House will find that it identifies a large number of risks in total. 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 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.

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

- A risk review: the management board considers all the operations and activities of the House in relation to its objectives and sets out to identify the associated risks at strategic level. Departments should then work on linking those strategic risks with its own departmental risks to build a risk profile for the whole range of House activities.

- Risk self-assessment: An approach by which each level and part of the House 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).

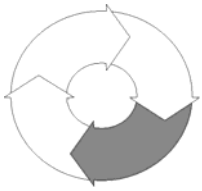
3.6 These approaches are not mutually exclusive, and a combination of approaches to the risk assessment process is desirable – this sometimes exposes significant differences in risk perception within the House. These differences in perception need to be addressed to achieve effective integration of risk management at the various levels of the House.

3.7 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.

3.8 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 departments ensure that they have comprehensively considered the range of potential risk which may arise; it also provides headings under which departments may choose to group their specific risks in their risk profile documentation. The table does not claim to be comprehensive - some departments may be able to identify other categories of risk applicable to their work.

CATEGORY OF RISK	Examples / explanation
1. External (arising from the external environment, not wholly within the House's control, but where action can be taken to mitigate the risk) *[This analysis is based on the "PESTLE" model – see the Strategy Survival Guide at www.strategy.gov.uk]*	
1.1 Political	Change of government, cross cutting Parliamentary decisions; Commission, Member, Committee decisions.
1.2 Economic	Ability to attract and retain staff in the labour market; financial constraints
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, procurement, accounting requirements
1.6 Environmental	Heritage site, buildings need to comply with changing standards; green issues,
2. Operational (relating to existing operations – both current delivery and building and maintaining capacity and capability)	
2.1 Delivery	
2.1.1 Service	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) HR (staff capacity / skills / recruitment and retention) Information (adequacy for decision making; protection of privacy) Physical assets (loss / damage / theft)
2.1.5 Relationships	Delivery partners (threats to commitment to relationship / clarity of roles) Customers / Service users (satisfaction with delivery) Accountability (particularly to HOCC and House as a whole)
2.1.6 Operations	Overall capacity and capability to deliver
2.1.7 Reputation	Confidence and trust which stakeholders have in the House
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
3. Change (risks created by decisions to pursue new endeavours beyond current capability)	
3.1 Change programmes	Programmes for Houseal or cultural change threaten current capacity to deliver as well as providing opportunity to enhance capacity
3.2 New projects	Making optimal investment decisions / prioritising between projects which are competing for resources
3.3 New policies	Policy decisions create expectations where the House has uncertainty about delivery



4. ASSESSING RISKS

4.1 There are three important principles for assessing risk:

- be clear about the difference between inherent and residual risk (see 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 which facilitates monitoring and the identification of risk priorities.

4.2 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.

4.3 This assessment needs to be done in respect of both <u>likelihood</u> of the risk being realised, and of the <u>impact</u> if the risk is realised. The House has adopted a "5x5" matrix with impact measured on a scale of "insignificant / minor / moderate/ major/ catastrophic" and likelihood on a scale of "rare / unlikely / possible / likely / almost certain". 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.

<u>Risk/tolerability matrix</u>

5	VH/VL (5)[1]	VH/L (10)	VH/M (15)	VH/H (20)	VH/VH(25)
4	H/VL (4)	H/L (8)	H/M (12)	H/H (16)	H/VH (20)
Impact 3	M/VL (3)	M/L (6)	M/M (9)	M/H (12)	M/VH (15)
2	L/VL (2)	L/L (4)	L/M (6)	L/H (8)	L/VH (10)

[1] Bracketed figures are risk exposures, i.e. impact multiplied by likelihood.

1	VL/VL (1)	VL/L (2)	VL/M (3)	VL/H (4)	VL/VH (5)
	1	2	3	4	5
	Likelihood				

4.4 At the organisational level risk appetite can become complicated 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 that impact. 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.

4.5 Thinking about risk frequently focuses on residual risk (i.e. - the risk after control has been applied which, assuming control is effective, will be the actual exposure of the House- 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.

4.6 However care should also be taken to capture information about the *inherent* risk. If this is not done the House 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.

4.7 Risk assessment should be documented in a way which records the stages of the process (see Annex 2 and HOC Guidance Notes). Documenting risk assessment creates a *risk profile* for the House 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.

4.8 Once risks have been assessed, the risk priorities for the House 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 House, and should consequently be considered regularly by the Management 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.

5. RISK APPETITE

5.1 The concept of a "risk appetite" is key to achieving effective risk management and it is essential to consider it before moving on to consideration of how risks can be addressed. The concept may be looked at in different ways depending on whether the risk (the uncertainty) being considered is a threat or an opportunity:

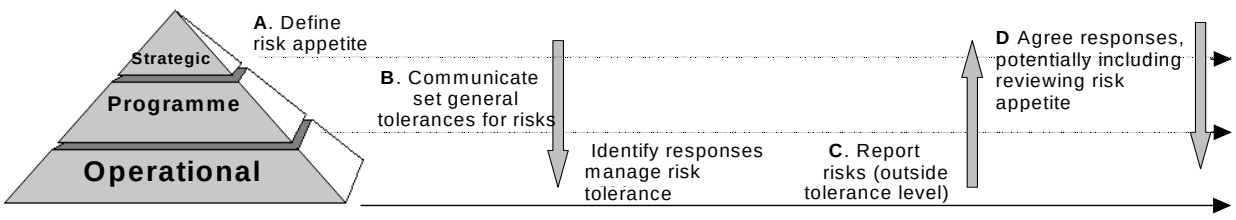
- When considering threats the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should it be realised. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance;

- When considering the opportunities the concept embraces consideration of how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. In this sense it is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses may be incurred with or without realising the benefits).

It should be noted that some risk is unavoidable and it is not within the ability of the organisation to completely manage it to a tolerable level – for example many organisations have to accept that there is a risk arising from terrorist activity which they cannot control. In these cases the organisation needs to make *contingency plans*.

5.2 In either case the risk appetite will best be expressed as a series of boundaries, appropriately authorised by management, which give each level of the organisation clear guidance on the limits of risk which they can take, whether their consideration is of a threat and the cost of control, or of an opportunity and the cost of trying to exploit it. This means that risk appetite will be expressed in the same terms as those used in assessing risk. An organisation's risk appetite is not necessarily static; in particular the Board will have freedom to vary the amount of risk which it is prepared to take depending on the circumstances at the time. The model below sets out these concepts in more detail:

Risk Appetite



5.3 The concept of risk appetite can be further analysed thus:

- **Corporate Risk Appetite**
  Corporate risk appetite is the overall amount of risk judged appropriate for the House to tolerate, agreed at board level (letter A above). This may not be just one statement: 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.

  The Board and senior managers have judged the tolerable range of exposure for the House and identified 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).

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

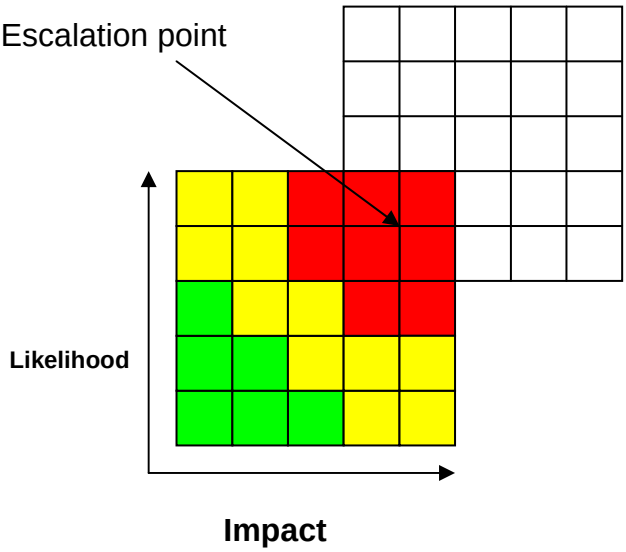
- **Project Risk Appetite**
  Projects that fall outside of day-to-day business of the House might need their own statement of risk appetite. Different types of projects might also require different levels of risk appetite, for example the House may be prepared to accept a higher level of risk for a 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
  b) Standard development projects: for example IT, procurement etc.
  c) 'Mission critical' projects: where the House needs 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).

5.4 Effective management and application of delegated risk appetite requires escalation processes. It is possible to set 'trigger points' where risks can be escalated to the next level of management as they approach or exceed their agreed risk appetite levels (letter C in the model at 5.2). 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).

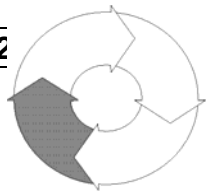


5.5 Further applications of the concept of risk appetite include:

- **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.

- **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.



6. ADDRESSING RISKS

6.1 The purpose of addressing risks is to constrain them to a tolerable level (i.e. – within the risk appetite). Any action that is taken by the House 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 (outsourcing i.e. PWC contract). 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 House 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 This option can be particularly important in project management if it becomes clear that the projected cost / benefit relationship is in jeopardy.

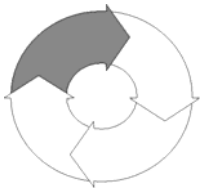
TREAT: By far the greater number of risks will be addressed in this way. The purpose of treatment is that whilst continuing within the House with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level. Such controls can be further sub-divided according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

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 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 House. 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 the House 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 the risk management process are reviewed at least once a year. Some aspects may need to be reviewed continuously.
- 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 House-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 House 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 the House'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 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 House. It

will have a wide ranging view of the whole range of activities which the House 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 House 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 The House Administration Audit Committee supports the Accounting Officer in his responsibilities for issues of risk, control and governance and associated assurance. The Audit Committee advises the Accounting Officer to:

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

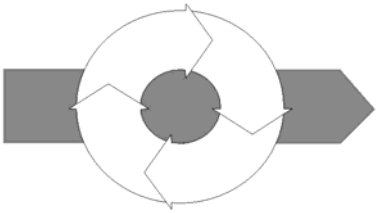
The Audit Committee should be asked by the Accounting Officer to

- comment on the appropriateness of the risk management process,
- receive reports on various aspects of risk management, and provide opinion and challenge,
- contribute to the process of assurance through regular attendance of risk owners at Audit Committee meetings.

7.6 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 House's risk profile.

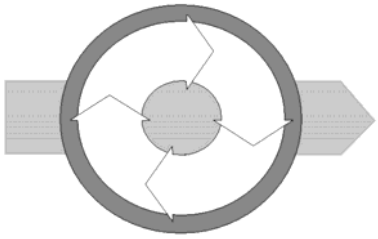
8.3 Communication within the House about risk issues is important:

- It is important to ensure that everybody understands, in a way appropriate to their role, what the House's risk strategy is, what the risk priorities are, and how their particular responsibilities in the House 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 department of the House 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, via the Office of the Chief Executive.
- 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 partners i.e. House of Lords/PICT about risk issues is also important (see also Section 9 – The Extended Enterprise), especially if the House is dependent on the partner not just for a particular contract but for direct delivery of a service on behalf of the House. 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 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 House is managing risk to give them assurance that the House will deliver in the way which they expect, and to manage stakeholder expectation of what the House can actually deliver.

9. THE EXTENDED ENTERPRISE

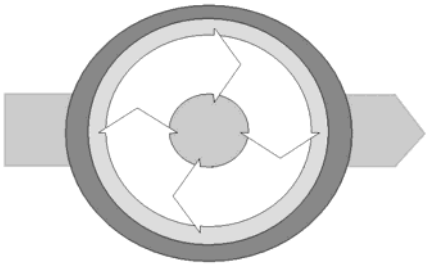


9.1 The House of Common is not entirely self-contained – it has a number of interdependencies with other organisations/stakeholders. These inter-dependencies are sometimes called the "extended enterprise" and will impact on the House's risk management, giving rise to certain additional risks which need to be managed. These considerations should include the impact of the House'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 have inter-dependencies with other organisations (e.g. in the case of HOC this is the House of Lords), 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 The House also has dependencies on contractors, although the extent of these dependencies will vary. These relationships may range from straightforward supply of goods which the House requires in order to function, through to delivery of major services to, or on behalf of, the House. This could include contracted out services such as cleaning. A particular potential problem here is when the House has a high dependency on a contractor, but the House is only a minor client for the contractor (for example, Price Waterhouse Coopers). It is important that Houses 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 House is permitted to take or address risk. Often the only response which the House can make in relation to the risk environment is to prepare contingency plans. For example, most public sector 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. It is important that the House considers its wider risk environment and identifies the way in which it impacts on its risk management strategy.

10.2 Laws and regulations, in particular Freedom of Information, can have an effect on the risk environment. It is important for the House to identify the ways in which laws and regulations make demands on it, either by requiring the House to do certain things or by constraining the actions which the House is permitted to take. For example, the way in which the House handles the risk of staff performing inadequately is constrained by employment legislation.

10.3 There is a particular strand of risk management which is important in providing the House with risk based procedural advice. Officials in the House may be constrained in the risks which they take into account.

10.4 The House is also constrained by stakeholder expectation. Risk management actions, which appear good value and effective in the abstract, may not be acceptable to stakeholders.

Annex 1

House of Commons Risk Management Policy and Strategy
Introduction

This document sets out The House of Commons policy and strategy for the identification and management of risk, including the roles and responsibilities of all managers and staff across the organisation.

Guidance and briefing on the day-to-day assessment and management of risk are set out in the House of Commons Risk Management: Guidance notes.

The policy on management of risk

The identification and management of risks affecting the House's ability to achieve its objectives are key responsibilities of all managers and staff of the House. The effective management of risk is an important means by which the House achieves its goals. To that end the House's policy is to:

h. manage risk actively across the full breadth of operations within the House.
i. devolve responsibility for risk ownership and risk management to the most appropriate local level within the House, but complementing this with oversight and monitoring mechanisms
j. integrate local risk management with local business planning (the business planning process is used to set objectives, agree action plan and allocate resources)
k. develop understanding of a risk–aware approach to working
l. provide and maintain guidance on the techniques of risk assessment and risk management
m. monitor and report regularly and frequently on the management of risk; and
n. keep policy and practice under review.

The key principles

The following key principles underlie the House's approach to risk management:

- This policy forms part of the House's corporate governance and internal control and assurance arrangements.
- Risk management is one of the key tools to ensure the achievement of the House's business objectives set out in its strategic Corporate and annual departmental business plans, and as such is an integral part of planning and monitoring.
- Risk management is a process for defining, analysing, controlling and managing risk.
- The Management Board is ultimately responsible for the internal control arrangements, including risk management.

The House defines risk as:

'The threat that an action or event will adversely affect the House's ability to achieve its current and future objectives.'

In its management of risk, the House makes a distinction between strategic (corporate) risk and operational risk. This distinction is reflected in the respective roles of the Management Board, second tier management groups (HRG, BPG) and Departments of the House.

- Operational risks are primarily to do with the day-to-day conduct of the House's business or the management of the House as an organisation – governance, staffing, resourcing, procedural and administrative systems. The management of operational risk is an integral part of business planning, management and monitoring, that has been delegated to Departments and, where appropriate, the second tier management groups.
- Strategic risks are different. They are invariably less to do with the day-to-day conduct of the business of the House and are more to do with the nature and purposes of the organisation, its ability to achieve its mission, the environment it operates in, the needs of Members of Parliament and other stakeholders and the reputation of the House. Strategic risks are identified and managed by the Management Board through its own annual assessment of risks. Key strategies for managing strategic risks include adaptability and responsiveness, working in partnership with stakeholders to understand and meet their needs, developing expertise so that the organisation can respond to change as circumstances alter.

Risk management strategy: roles and responsibilities
Role of the Management Board

The Management Board has ultimate responsibility for the management of risks. It monitors the approach to the management of risk, and its effectiveness in managing risk and the implementation of this risk management policy and reporting requirements. It considers the risks facing the House at a strategic level. Its role includes:

a. instilling a culture of risk management:
b. satisfying itself that risks are managed appropriately:
    - identifying emerging strategic risks;
    - approving the overall risk management arrangements;
    - monitoring the management of significant risks;
    - satisfying itself that the less significant risks are being actively managed, and that the appropriate controls in place are working effectively;
    - annually reviewing the approach to risk management and approving key changes or improvements to processes and procedures.

Role of the Audit Committee

As part of the Audit Committee's role to advise the Accounting Officer on the effectiveness of the House's internal control arrangements, it will:

c. annually review the House's approach to risk management and overall risk management arrangements
d. advise the Accounting Officer on the implications of internal audit reports and the recommendations made by the external auditors.

Role of the Office of the Chief Executive

The Risk Facilitation function resides in the Office of the Chief Executive (OoCE), which supports the Clerk in his role as Chief Executive of the House of Commons. Under the direction of the head of OoCE the House's risk facilitation team is responsible for:

- maintaining the House Risk Management policy, strategy and guidelines;
- facilitating the Management Board in its annual identification and assessment of the strategic risks faced by the House and the updating of the corporate risk register;
- overseeing the assessment of operational risks (at departmental level) and the preparation of risk registers; and
- preparation of reports to the Audit Committee and the Management Board.

Role of the Director Generals

Their role is to identify, assess, manage, monitor and report on the management of operational risks at the Group level. Specifically, as part of the development of local operating plans. Director Generals are responsible for:

g. devising an appropriate local mechanism for identifying, assessing, managing, monitoring and reporting on risk which reflects the House's risk management policy;
h. implementing policies on risk management and internal control arrangements at the departmental level;
i. as part of the annual business planning exercise describing risks identified and how they are being managed in accordance with the House's risk management guidelines;
j. identifying, assessing and developing a strategy to manage risks for the objectives set out in the departmental business plans;
k. monitoring the management of the risks for which they are responsible; and
l. providing adequate information to the Management Board, the status and management of risks.

Role of staff

All employees of the House are expected:

- to be familiar with the House's policy on and approach to risk management ;
- to take a risk management approach to their work;
- to take responsibility for the risks they 'own;'
- to highlight ways in which the business objectives may be at risk and could be managed better; and
- to consider how the House might reduce its exposure to risk.

Risk management as part of the system of internal control

The system of internal control incorporates risk management. Together, a number of elements facilitate the effective management of risks. These elements in the House include:

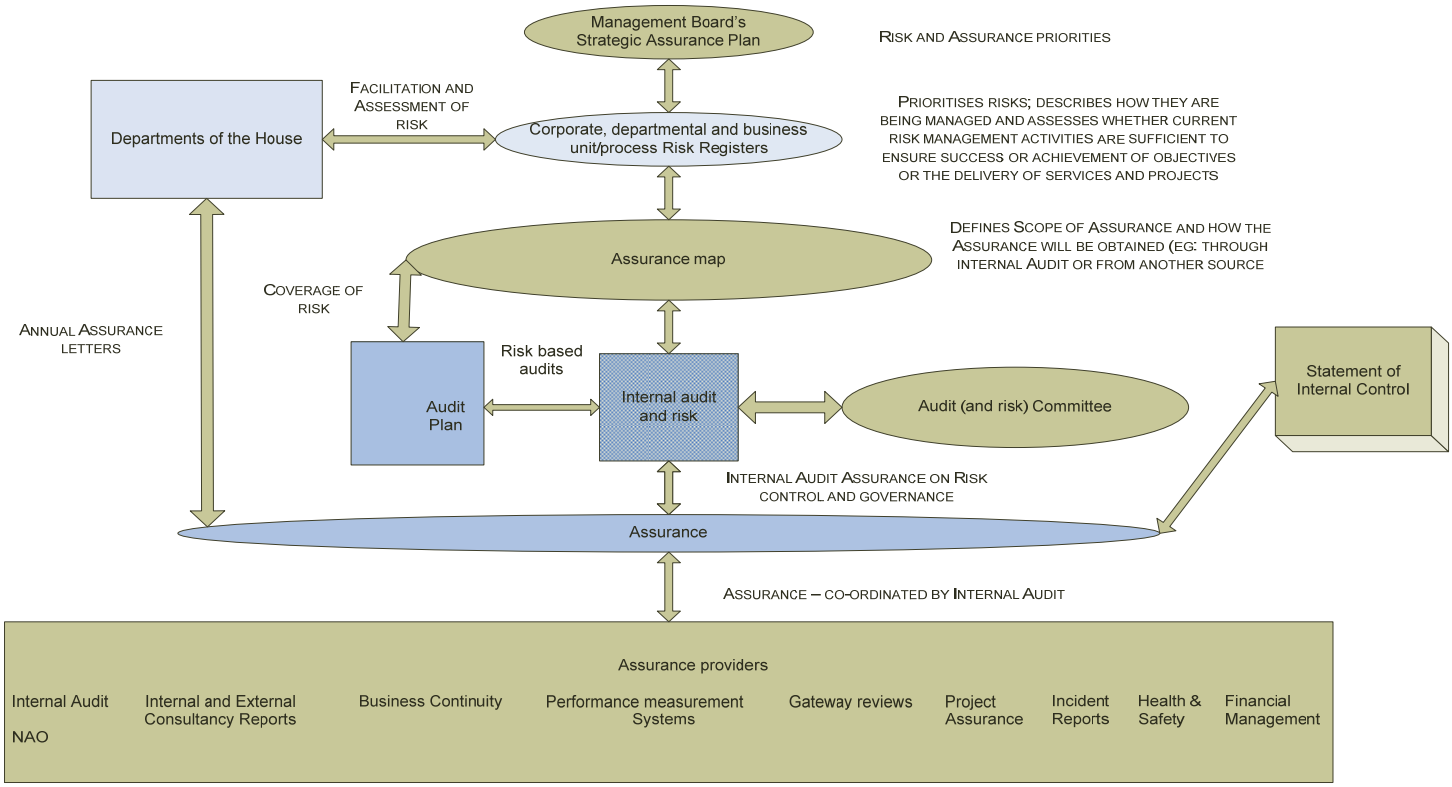
- risk management policies and procedures
- Comprehensive reporting to monitor key risks and their controls
- Business Planning Process used to set objectives, agree action plans and allocate resources
- Corporate risk register
- Departmental risk register
- Audit Committee
- Internal Audit
- External Audit
- Other sources of assurance within the House, e.g.: Health and Safety, specialist consultants etc; will increase the reliability of the system of internal control.

Annex 2
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 3

Assurance Model on Risk Management



Annex 4

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