MANAGEMENT BOARD
Risk Management Audit Report 2008/09

Paper from the Corporate Risk Management Team (CRMT)

Purpose of paper

1. This note updates the Management Board on the 2008/09 Internal Audit (IA) risk assurance audit report (issued under separate cover) which includes the preliminary management response by the Head of the Office of the Chief Executive (the Audit Sponsor - Annex 3).

Action for the Board

2. The Board is asked to take note of the findings and are invited to give any views to the CRMT at the next round of corporate risk review meetings scheduled for the beginning of the summer recess.

Main Audit Findings

3. The main audit findings, identified in the report, require the CRMT to address the following issues:
    a) to ensure that the organisation is open and transparent about those significant events that have an impact upon the assessment of the Corporate risks (para 7 IA);
    b) to embed the CRMT in organisational reporting structures to ensure that they receive timely and detailed information on any events that relate directly to the top ten corporate risks and the management of those risks (para 7 IA);
    c) to improve the existing information in the departmental risk registers on mitigations (para 11 IA);
    d) to revisit the HoC risk management policy to ensure it remains appropriate for the House; the audit report suggests (para 22 IA) that we consider lowering our risk management aspirations from being a “risk enabled” to a “risk managed” organisation;
    e) to promote and embed the policy in a way that makes it real for the people who are managing risk, to ensure they are aware of the benefits good risk management can bring (para 25 IA);
    f) to work with managers to ensure they are actively managing risk, this will involve a more “challenging” role by the CRMT (para 27 IA); in practice this may meeting risk owners on a more regular basis (possibly monthly).

4. The CRMT will take forward these issues over the summer recess. A full response and action plan will be developed for the consideration of the MB in September 2009 and, subject to the MB’s approval, reported to the Audit Committee in October 2009.

Rachel Harrison/ Dermot Woods
Corporate Risk Management Team
July 2009

Internal Audit
Office of the Chief Executive

House of Commons

Internal Audit 08/09

Review of Risk Management

Final Report

Audit Sponsor:	Philippa Helme, Head of the Office of the Chief Executive (OCE)
Copied to:	Administration Estimate Audit Committee members Rachel Harrison, Corporate Risk Facilitator, OCE Dermot Woods, Assistant Corporate Risk Facilitator, OCE Paul Thompson, Head of Internal Audit, House of Lords Helen Booth, Director, National Audit Office
Date of issue:	7th July 2009 (Final) 25th June 2009 (draft v2) 8th June 2009 (draft v1)

Internal Audit of Risk Management (2008/09)

Background and introduction

1. The House has adopted a central Risk Management Policy and Strategy, together with Principles and Concepts, that sets out how the system of risk management will be operated. A policy has been in place since 2001, based on best practice as advised by HMTreasury.[1] PICT adopted its own risk management policy in January 2009, which closely aligns to the House of Commons Risk Management Policy.

2. Risk management, as a discrete and systematic management approach, has been on a continuous course of implementation and refinement in the House. The House of Commons Risk Management Policy and Strategy have been adopted by the Management Board, and the area has been the subject of internal audit reviews in previous years.

3. This audit is a key element towards the Head of Internal Audit's opinion for 2008/9 and hence the Accounting Officer's Statement on Internal Control. The broad scope of the audit was to determine whether the system of risk management is operational at corporate and departmental levels

Audit Approach

4. The audit assessed the following steps in the risk management process:

   Risk Identification: That all Principal Risks to the achievement of objectives, priorities and aims of the House, have been identified and recorded on a Risk Register

   Risk Assessment: That all Principal Risks have been assessed at Inherent level, in terms of their Impact and Likelihood, on a consistent basis

   Risk Management: That the method for the effective management of each individual risk has been appropriately documented and recorded in the Risk Register, in terms of both design and operation

   Effectiveness of the management of risk: That an assessment of he effectiveness of the management of each risk, in terms of design and operation, has been carried out and recorded in the Risk Register as an assessment of the Current (or residual) Risk, in terms of Impact and Likelihood

[1] Management of Risk – A Strategic Overview H M Treasury Jan 2001

Remedial Action Plan: That any gap between the assessment of the Current risk level assessment and the desired level of risk (the Target risk level or risk tolerance) has an associated management action plan that will mitigate the gap

Monitoring and reporting: That all Principal Risks are being reported to, or monitored by, an appropriate individual or group with the authority to initiate remedial action

5. An audit testing programme was developed covering these areas, and was used for an informal update earlier in the year. The results were shared with members of the Corporate Risk Facilitation Team (CRFT).

6. The audit was undertaken using, primarily, techniques of observation and enquiry, together with the examination of documentary evidence.

Conclusion and Main Findings

Recent Developments

7. Over the past year there have been significant moves forward in a number of areas:

Management Board

- The review of the Top Corporate Risks in November 2008

- The reporting of the status of the corporate risks in the Corporate Balanced Score Card with an executive summary covering significant risks and horizon scanning information outlining emerging or increasing risk areas for the Management Board's attention. Target risk scores will also be reported in the Balanced Score Card

- The introduction of escalation procedures and the reporting of 'Board' or corporate principal operational risks to the Management Board, which allows discussions at Board level about the risks which sit marginally below the corporate level

Departments

- Departments can now escalate significant or emerging risks to the Management Board

- PICT has published its own risk management policy, standards and guidance. There is a clear policy statement which explicitly sets out what PICT will put into place and do to manage its risks. Other Departments should be

encouraged to explain and agreed with the CRFT how they will implement the House Risk Management policy

- PICT has identified target risk scores in its risk register and mitigations have been assigned owners

- The reporting of 'top risks' is a regular agenda item (either

  monthly or quarterly) for the senior management groups in all Departments

- Departments have their own risk co-ordinators, usually one of their own business managers to co-ordinate and regularly update their respective risk registers and to liaise with the CRFT and attend the Corporate Risk Forum

- We found evidence of departmental risk management workshops; consultation exercises and one to one meetings to identify and score risks; consolidate risks where there was duplication and to review controls.

Corporate Risk Facilitation Team

- One additional full time professional risk resource has been assigned to the CRFT

- There is proactive communication between the CRFT and key staff, stakeholders and management groups in the House (eg: the Business Risk and Resilience Group, and Fire and Health & Safety officials). More still needs to be done to ensure that the organisation is open and transparent about those significant events that have an impact upon the assessment of the Corporate Risks. There is a need to embed the CRFT into organisational reporting structures to ensure that they receive timely and detailed information on any events that relate directly to the top ten corporate risks and the management of those risks. A recent example was the Canon Row power failure and the failure of back up generators in the Easter 2009 recess. Corporate risk 2b covers utility failure. The CRFT were not directly or formally told about the power failure and its impact in order to update the Corporate risk register

- Improved sharing of corporate knowledge about risk with the creation of the Risk Forum, a newly formed risk management support and information/best practice sharing group

- The development of the 'shared area' \\hpap03f\CrossDept which will help to manage the information flow across the risk

community, in particular, for the escalation of Board risks and the review of Departmental Risk Registers

Current Developments

8. Further house-wide developments are also evident, for example the revision of the 'Principles and Concepts' guidance into a more user friendly and practical guide to risk management (due to be available later in 2009)

9. The CRFT are working with PricewaterhouseCoopers to improve the capture and recording of information about the key mitigations relating to the corporate risks

Review of Main Findings

10. Departments follow a systematic risk management process, although there is some inconsistency in its application. The design of these processes was found to be sound, since they were generally based on the HM Treasury risk management model.

11. Overall, the quality and accuracy of the information in the risk registers varied between departments. Good practice was found at the corporate level, which is co-ordinated by the CRFT, and also in PICT, Facilities and DCCS, but we felt that more work is needed to improve the information in the registers on how the risks are being mitigated; in terms of the identification, documentation and evaluation of key controls and planned mitigations.

12. Director Generals are responsible for devising appropriate local mechanisms for identifying, assessing, managing, monitoring and reporting on risk which reflects the House's risk management policy[2]. In practice this has resulted in a variety of approaches being taken by departments. A balance between the benefits of standardisation and local application needs to be struck, but there also needs to be an ability to ensure that the systems in place by DGs are challenged about their effectiveness

13. Risk Management is viewed, by some managers that we talked to, as a process or a series of tasks principally focussed on the completion of the Corporate and Departmental risk registers, with information supplied by corporate and departmental risk owners. While this captures a high proportion of the strategic and operational risks it, should then be used to review and improve the management of risks. If the risk registers are not sufficiently complete and accurate, it does not provide the complete risk profile for the organisation that can be used to lead improvements.

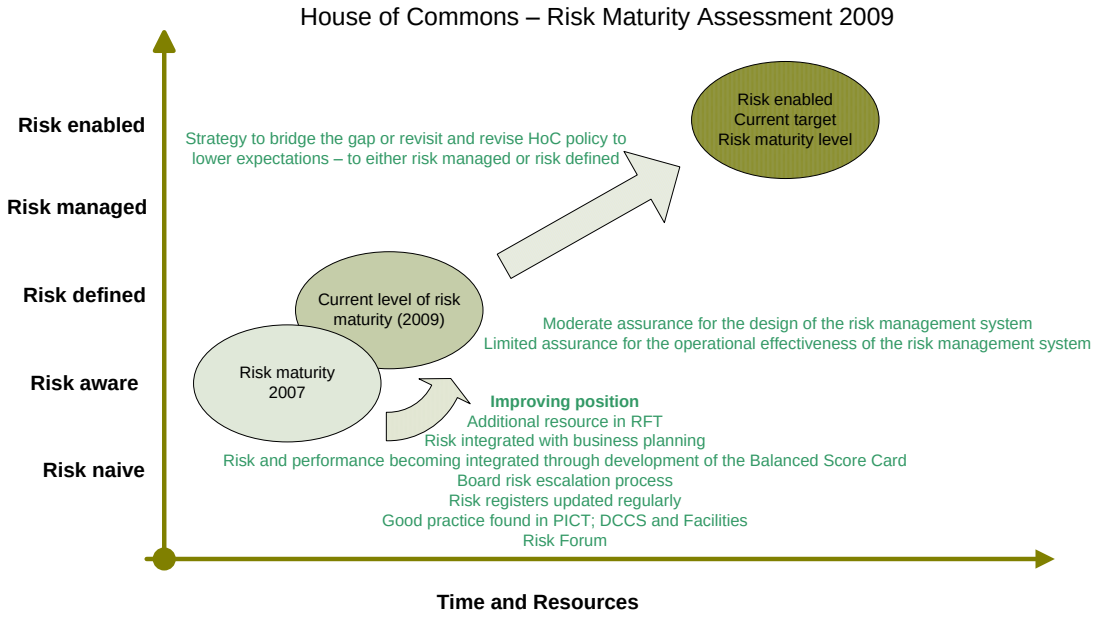
[2] House of Commons Risk Management Policy and Strategy (not dated)

14. There is a mixed picture regarding the how management gain the benefits that should emerge from the system of risk management. Principally this is looking at the assessment of the effectiveness of the management or mitigation of risks, but should then be supported by accurate monitoring and reporting of risks that lead to appropriate interventions. From our review Departments were poor at assessing the effectiveness of controls and mitigations, so that judgements were found to be based on 'gut feelings' rather than more tangible evidence. Without a more systematic approach, that challenges 'gut feelings' the ability to identify and drive improvements, which is the benefit of good risk management, is lost.

Risk Maturity Assessment

15. Our assessment of the risk maturity of the House is that the House is **Risk Defined**, where strategies and policies are in place and communicated and the risk appetite has been defined in some areas.

16. The diagram below shows that there is some way to go before risk management is fully embedded in the House, in line with the adopted policy. The criteria used to assess organisational risk management maturity was defined by the IIA-UK in a position statement issued in 2003. The scale starts at risk naïve (where an organisation is assessed as having no formal approach developed for risk management) to, at the top of the scale, risk enabled (where risk management and internal control are fully embedded in operations). A fully risk enabled organisation would proactively and effectively manage uncertainty and maximise the benefits from risk management. From our knowledge and that from other organisations, very few (if any) organisations in the public sector are at this level of risk maturity.



17. Our risk maturity assessment shows and recognises the step change in the progress made since the last full audit of the House's risk management arrangements, which was performed by PricewaterhouseCoopers (PWC) in 2007. It is clear that the direction of travel has been positive and that the risk management process has been enhanced and improved over this period. We followed up progress with the recommendations made in the PWC report, and found that significant progress has been made in addressing:

- resourcing levels to support the ongoing development of risk management
- updating the risk management policy
- the consideration of risk tolerance by the Management Board
- escalation of significant operational risks to the Management Board
- the consistent use of heat maps
- improving awareness of risk management through presentations at induction training for new staff; the Managing for Excellence programme and at other events

Issues to be Considered

18. A number of fundamental issues should be addressed before the House will realise the full benefits of effective risk management:

Is the House's vision for risk management right?

19. The risk management policy has been the key driver behind the House's undertaking to embed risk management. The challenge has been not just to design appropriate processes, but to ensure that they

become properly embedded into the operation and the culture of the organisation and so lead to improvements.

20. Very few, if any, organisations have achieved the level of risk maturity envisaged in the formal policy. For many, the benefits of achieving the ultimate level of risk maturity have not outweighed the cost to get there.

21. Our review suggests that the House has reached a critical decision point with regard to the future focus of risk management and whether it should continue to strive to reach a level of risk maturity that may not be achievable or even desirable, within the existing culture and the level of engagement with risk management.

22. A possible next step would be for the Management Board to revisit and revise the current risk management policy with a view to lowering its risk management aspirations from being a "Risk Enabled" (where fully embedded risk management is integrated with all other management activities) to a "Risk Managed" organisation (where an organisation wide approach to risk management is developed and maintained, but is not wholly embedded with all other systems). We have set out some of the basic characteristics of a Risk Managed organisation in Annex 1.

Leadership and Direction of Risk Management

23. The CRFT are focussed on the identification and assessment of risks; seen in facilitating the Management Board in the annual assessment of strategic risks and the updating of the corporate risk register; overseeing the assessment of operational risks (at departmental level) and the preparation of risk registers; and the preparation of reports to the Audit Committee and the Management Board.

24. Their role is about facilitating the "system and processes" of risk management, and not necessarily about driving the improvement of the way that risks are managed to gain tangible benefits. This latter role is, quite rightly, one for line management.

25. We believe that there are three issues that need to be addressed, which are:

- there is a need for a senior individual with authority to give leadership and direction to both the work of the CRFT and nominated managers in Directorates, in the implementation of systematic and effective risk management
- the need for clarity about the role and responsibilities of the CRFT, in terms of the delivery of the House Risk Management Policy and leading the realisation of its full potential benefits

- Implementation of the House Risk Management Policy and the realisation of the potential benefits should be treated as a corporate key project and should be project managed. There is a need for an end date for when the appropriate level of risk management will have been achieved

26. Achieving these will ensure that the House realises the full potential benefits of risk management and will enable the House to:

- make better decisions,
- better deal with anything that could damage the House's reputation
- improve performance and service delivery,
- effectively manage change,
- make the most effective use of resources,
- minimise waste, fraud and poor value for money.

People, knowledge, skills and support

27. From our discussions with Risk Co-ordinators, we found their primary focus to be on the completion of their respective risk registers and not necessarily on the improvement of the management of risks. There was a view amongst this group that there were real problems in engaging Directors and Managers in risk management. As we have said in Paragraph 24, managers are key to driving improvements in the way risks are managed and the House needs to find a means for ensuring that managers are committed to its use. This will be achieved in part by ensuring that there is better understanding amongst managers of the purpose of risk management and its benefits. The challenge is in making sure this happens.

28. The risk management facilitators can take a more pro-active approach amongst the risk community, and look to focus their attention more on challenging and supporting the fundamentals of risk management, than on the process. To do this they should look for practical examples of benefits realisation.

29. Departmental risk co-ordinators are business managers who are experts in their own department's business and/or financial planning activities, and are also taking on more administrative functions under the re-modelling programmes. In general, although they are not experts in risk, they are expected to champion and implement a sound risk system in their respective departments. Risk co-ordinators, can make a difference to the effectiveness of risk management but this needs to be seen as an integrated part of their whole job, and for this they need the skills, tools and professional support and advice to do so, on a par with

the support provided by other professions, such as Human Resources or Finance.

Audit opinion

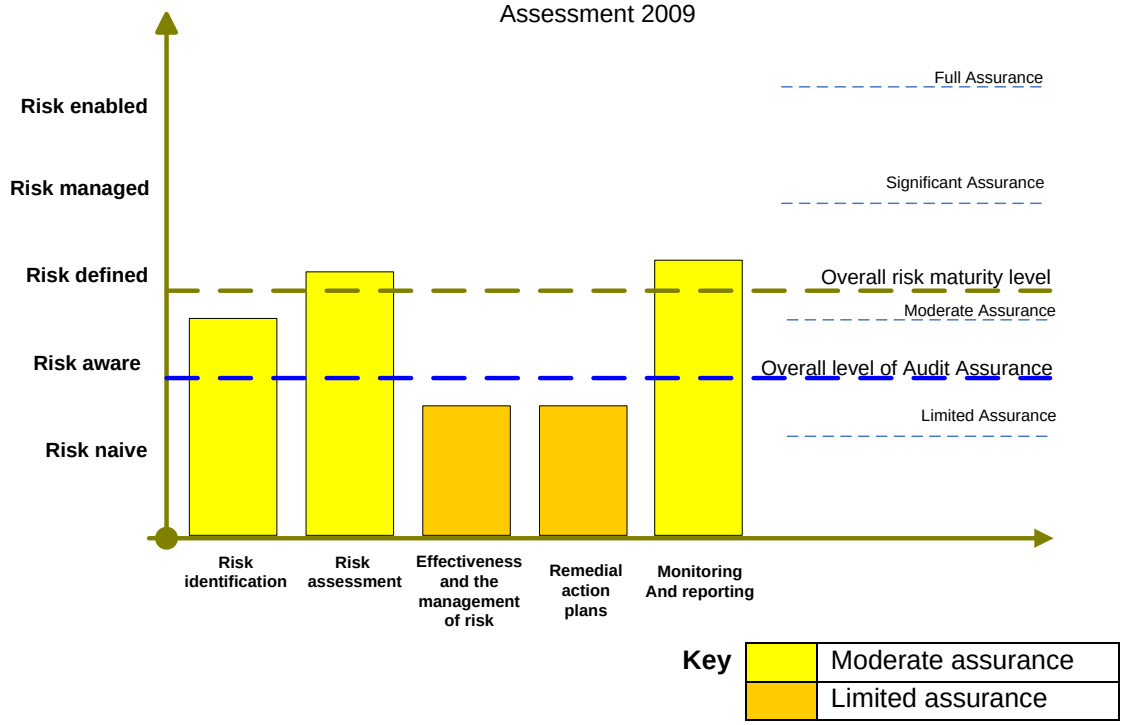
30. We have assessed the House's risk maturity as Risk Defined. There is a corporate risk register and departments have compiled lists of risks but it is possible that departmental risk registers are not complete. We have set out a number of development options in table 1 that would improve the current risk maturity level.

31. There are some weaknesses in the design and/or operation of controls; and because the quality of risk management and the level of engagement varies across the House the likely impact of these weaknesses on the achievement of the key system, function or process objectives is significant. Furthermore, these weaknesses are likely to impact upon the achievement of organisational objectives.

32. We therefore give a **Moderate** assurance opinion on the adequacy of the design of the system and a **Limited** assurance opinion on the operating effectiveness of the system and controls in place over risk management at the time of our audit.

33. The combination of these opinions are illustrated below :

House of Commons – Risk Maturity and Audit Assurance Assessment 2009



34. **Next Steps – What should happen next?**

- The Management Board should review the current risk management policy and its aspirations for risk management
- Strengthen senior level leadership and direction for both the work of the CRFT and nominated managers, in the implementation of systematic and effective risk management
- Clarify the role and responsibilities of the CRFT, in terms of the delivery of the House Risk Management Policy and leading the realisation of its full potential benefits, with less focus on process and more on the value of risk management
- Implementation of the House Risk Management Policy and the realisation of the potential benefits should be treated as a key corporate project that is project managed. A project plan should be put in place to deliver the HoC risk management policy and the Management Board's aspirations.

35. In the next section (table 1) we give our audit assurance for each key step in the risk management process, along with a summary of the evaluation criteria and a summary of our findings. In Annex 1 we have summarised the good practice found in the House and set out a number of development options that would improve the current level of risk maturity. In Annex 2 we have extracted some key characteristics of a risk managed organisation from the OGC risk management strategy and the guidance in Risk: Good Practice in Government [3].

36. The management response to this audit, in a paper to the House of Commons Administration Estimate Audit Committee (July 2009) is reproduced in Annex 3.

[3] published March 2006, by HM Government ISBN 10 1-84532-149-9

Table 1	Evaluation Criteria	Evaluation summary – see also Annex 1 for details of good practice found in the House and areas for development
Risk identification Design: Moderate; Operation: Moderate	Objectives set out in the corporate business plan	The Corporate business plan sets out the aims and priorities for the House Administration. The plan sets out the broad strategic direction for the development of services to achieve the core tasks. Historically a bottom up approach has been taken, which means that departmental rather than strategic priorities drive the corporate plan – but this is changing!
	Corporate and strategic risks identified	The Management Board's ten corporate risks and details of the Board level risk owners are published in the corporate plan
	Principal risks are not missing or duplicated	Departments were not able to confirm what mechanism's are in place to ensure that all principal risks are recorded in their respective risk registers. Evidence of workshops, one to one meetings but no evidence of systematic identification of risk such as CRSA approach. No evidence of the categorisation of risks except in PICT
Risk assessment Design: Significant; Operation: Limited	Standard assessment criteria is in place	A standard assessment criteria is in place (5 x 5 scale); guidance is set out in the principles and concepts. PICT guidance explains with examples the numerical values for impact and likelihood. Departments could not confirm that the risk assessment matrix had been used consistently – assessments were based on 'gut feelings'
	The standard assessment criteria is used consistently	Risks on the Corporate and departmental risk registers are given a numerical rating for both inherent and residual risk – based on the perceived exposure for likelihood and impact. A total risk score is the product of these two figures and determines the colour coding of the risk on the 'heat map'
	Risks of a similar nature have been consistently assessed	The scores of similar risks were analysed and compared by Internal Audit. The analysis showed that similar risks were not consistently scored. Where corporate risks were also recorded on departmental risk register the scores for the security and staff risks were the most consistent (although there were some differences) the least consistently scored were IT risks.
Effectiveness of risk management Design: Moderate; Operation: Limited	Entries in the risk registers are complete and accurate representation of the main ways that the risk is being managed (design)	The quality of risk registers varied from department to department. There was evidence that a number of risk registers were incomplete. The quality of the information relating to controls and mitigations also varied.
	The options to Treat, Transfer, Terminate or Tolerate or Take are clearly set out	The options are set out in the principles and concepts. There was no evidence that discussions regarding the mangement of risks and the development of mitigations considered the 5T's. The approach taken was generally always to Treat; identify what was being done within the organisation and then link these to a risk, rather than consider what needs to be done or what should be done differently to effectively manage a risk
	Entries in the risk registers are complete and accurate representation of the main ways that the risk is being managed (operation)	No reference is made to the design, operation or effectiveness of the mitigations or whether things need to be done differently, or if less or more is required. The area of measuring the effectiveness of mitigations should be addressed as risk scores in the RRs tend to be static

Table 1 continued

	Evaluation Criteria	Evaluation summary – see also Annex 1 for details of good practice found in the House and areas for development
Remedial Action Plans Design: Moderate Operation: Limited	A target risk level has been set for each risk, representing risk appetite/tolerance in terms of allowable impact and likelihood	The organisation has not developed a risk appetite/risk capacity framework from within which it manages its risks. Target risk levels are in development for the Corporate Risks and will be reported in the Balanced Score Card. PICT identified target risk scores for its principal risks
	Any gap between the current risk assessment and the target risk assessment has a remedial action plan	Mitigations identified but generally not with the aim of reaching a target risk score. Not all risks in the departmental risk registers had mitigations identified against them. Mitigations had 'ongoing' target finish or implementation dates
	The risk owner confirms that the remedial action plan is deemed to be satisfactory	No evidence that this practice was in place
	Corporate risks are being reviewed by the Management Board and action is being seen to be taken as warranted	The Management Board are actively engaged in reviewing corporate risks when 'board risks' are escalated to the Management Board either by the CRFT or by departments. The Management Board minutes show that there are discussions about risks eg: scoring of IT risks and the impact of the current economic situation on suppliers used by the House Administration. Not possible from the evidence available to substantiate if the risk/performance information has lead to improved or better informed decision making by the Management Board. No evidence of assurance being given to the Board on the effectiveness of mitigations and or action being taken – need Assurance frameworks development for each principal(important) risk
Monitoring and reporting Design: Moderate Operation: Moderate	Significant risks are being reviewed by the Management Board and action is seen to be taken when warranted	The management Board receive monthly information about Corporate risks and when Board risks are escalated. Departments can escalate new or emerging risks to the MB – mainly PICT risks, so far, with one from Resources. This is not systematic; there is no criteria for when departments should escalate risks to the Management Board
	A process exists to escalate or demote risks to a lower level of reporting/monitoring	Yes procedures are in place. In practice corporate risk are reviewed and remain on the risk register until the next annual (or six monthly review?), there is little movement in these risks either on or off the corporate risk register, although some of the risks have been spilt over time. The risks escalated by departments are not a fixed risk register, they appear for on the MB agenda and then disappear.

Annex 1

Policy Good Practice found in the House	Risk management policy in place (revised in 2008) and owned by the Management Board[4] PICT have own risk management policy owned by the PICT Board[5] Key principles and concepts for risk management defined for the House of Commons[6] - based on HMT Orange book and supporting guidance Key principles and concepts for risk management defined for PICT[7] Standards defined for risk management in PICT Roles and responsibilities defined for key stakeholders	**Potential areas for development**	Establish appropriate governance for risk management in the House – should the risk management agenda be delegated to House of Commons Administration Estimate Audit Committee – acting as a risk committee? This has been done in other organisations on a "task and finish" basis. Revisit the House of Commons risk management policy to establish if it correctly identifies the House's end vision for risk management and whether it is achievable Agreement of an end vision for risk management which sets out in clear terms where the House wants to get to with risk management (eg: fully embedded or enterprise wide risk management or a simpler risk management operation) Once the vision is agreed then a strategy and development plan should be put in place to take the House from where it is now to where it wants to be with risk management, over a defined timescale Promote the House's risk management policy in an integrated fashion with other management re-modelling initiatives. Message should come from the Management Board that having a formal risk management process for all to consistently follow is an essential part of good management

[4] House of Commons risk management policy and strategy, policy and guidance - 2008
[5] PICT risk management policy – January 2009
[6] House of Commons Risk Management Principles and Guidance – June 2008
[7] PICT guidance (Policy, concepts and principles and standards including ICT risk Management – 2009)

			Development of House standards and practical guidance that supports the risk management policy Improve accessibility to guidance Develop training programme to raise awareness of risk management standards and the House's approach (developing a risk aware organisation) and to ensure that staff understand their roles
Risk Identification Good practice in the House	Corporate plan identifies and states objectives and priorities and aims of the House[8] Management Board have identified ten corporate risks with designated risk owners who are members of the Board.[9] These risk relate to the delivery of the corporate business plan and are viewed as top down risks Risk identification is integrated with the business planning process[10] Risk classification guidance is set out in HoC Guidance. Risks are classified at a Corporate level. PICT identify risks in the broad classifications of operational, programme and project risks	**Potential areas for development**	Standard Risk Register template developed and then compliance enforced Evaluate the option of establishing a single risk register for the organisation (corporate and departmental risks held on the same risk register) – so that cross cutting risks are on the risk register only once (cross cutting risks eg: security appear on each departmental risk register), and that departments work collaboratively to manage the risks rather than in their departmental silos The Risk Register is accessible to all, so that individuals identifying risks are able to add information to the risk register Improve information links between RFT and other Groups (that sit outside of the corporate and departmental risk management process) for example: Resources Management Group; BRRG; recently formed Bi-cameral Swine flu pandemic management and planning group or the Corporate Gateway Review Team to ensure that risk registers are updated, if appropriate, and that a complete risk profile is built for the organisation

[8] House of Commons Corporate plan – March 2009
[9] House of Commons Corporate plan – March 2009, page 7
[10] Departmental business plans

	Risk Registers maintained by departments, which are updated monthly or quarterly. [11] Evidence of workshops eg in the Department of Facilities ; and meetings with risk owners Risk Facilitation Team (RFT) in the Office of the Chief Executive (OCE) provide professional advice and support to the management board and also to departments of the House Evidence that some management groups that sit outside of the corporate and departmental risk management process eg: Business Risk and Resilience Group (BRRG) are working in a risk based way and are linking in with the Risk Management Facilitation team (CRFT)		Departments identify operational risks Departments show their contribution to the management of the Corporate risks
Risk Assessment- Good practice found in the House	Each risk assigned and scored by a Risk Owner Standard 5 X 5 Matrix used by all departments Risks assigned a score based on a combination of the likelihood of occurrence and the probable impact should the risk happen Residual risk scores take account of the controls in place to reduce the likelihood of a	**Potential areas for development**	Criteria established and examples made available to help departments assess risks, the PICT Business Impact Reference Table is a useful model Establish mechanisms to improve the consistency in the scoring of cross cutting risks such as IT risks Risk scores should be regularly challenged by the RFT Target risk scores defined for all risks on the risk register

[11] Departmental risk registers - \\hpap03f\CrossDept\Board Performance Information

risk materialising or to minimise its impact should it happen

PICT gives specific guidance on the analysis of threats and vulnerabilities (Business Impact Reference table)[12]

Risks scored consistently within departments

The key threats or causes have been identified for the risks on the corporate risk register; the risks on the DCCS;DIS; Resources and the facilities risk registers

Most departments identified the some of the key controls that were in place to manage risks

Target risk scores identified for the corporate risks and also for the risks on the PICT risk register

[12] PICT: principles and concepts, Risk management- January 2009

Effectiveness and the Management of risk – Good Practice found in the House	Departments identify mitigations and planned mitigations to treat risks. Mitigations have designated owners Monthly mitigation updates were performed in most departments and risk registers updated. Progress is followed up and delays challenged	**Potential areas for development**	The quality of mitigations set out in the risk registers should be improved as this is how departments demonstrate that they are effectively managing their risks. This should identify all of the significant methods The effectiveness of mitigations/controls in actually managing the inherent risk should be reviewed, evidenced and measured as part of a strong scrutiny process which is linked to wider performance management arrangements Residual risk scores should not be static in the short, medium or long term if the risk is being effectively managed by the mitigations Assurance frameworks developed for each significant risk to provide evidence of the effectiveness of controls and mitigations
Remedial action plans – Good practice found in the House	Corporate and departmental risk registers show the planned mitigations	**Potential areas for development**	Performance indicators should be developed and reported on for planned mitigations Action plans should be developed with dates and those responsible and a commitment that the action will lessen the risk proportionately Action plans should be challenged as to their effectiveness and cost-benefit

Monitoring and reporting – Good Practice founding the House	Variety of reports used to report risk. Red, amber, green system and heat maps used for the reporting of risks Risk monitoring and reporting is becoming a regular feature of the performance management process with the development of the Balanced Score Card Board risks are reported to the Management Board on a monthly basis – where operational risks can be picked up by the Board Board debate risks for example Corporate risk 9 was discussed in March following the presentation of the Librarian horizon scanning paper with regard to anticipating the needs of new Members Risk is an agenda item for the Management Board and the management teams in departments – particular good practice was found in Facilities Escalation process in place for Departments to escalate increasingly significant risks to the Management Board for example PICT escalated its supplier risk to the Management Board in April All departments had mechanisms in place for reporting their top risks to their senior management groups or Directors
Potential areas for development	Further development of the Balanced Score Card to fully integrate risk, performance and assurance reporting for the Board Clear criteria for when departments must escalate risks to the Management Board Encouragement for the Management Board to demonstrate decisions and actions taken after discussing risks.

Annex 2

Characteristics of a Risk Managed organisation, or what does good risk management look like?

Definition of risk managed –Enterprise wide approach to risk management in place and communicated, but not necessarily wholly integrated into a fully embracing and integrated management approach

The following have been extracted from Risk: Good Practice in Government, published March 2006, by HM Government ISBN 10 1-84532-149-9 and the OGC risk management Strategy

1. Have the right people leading risk management
2. Simple but structured approach, not heavy on process; management at every level understands it and also understands what is expected of them
3. Consistent approach, no one has to re-invent the wheel!

4. There is clear accountability for managing risks
5. Clear structure in place to manage risks based on openness and transparency about what the big problems are and how to fix them
6. Communication strategy in place to sell the benefits of risk management – particular areas are targeted within the organisation eg: where there is the least engagement by managers with risk management
7. Mangers understand the benefits of risk management
8. Staff have the right tools to identify risks and their root causes
9. Risks are analysed simply and presented to the decisions makers; risks are clearly defined
10. Risk judgements are based on sound information
11. Staff on the ground are involved – key risks will often be spotted at this level; but risk management reaches right across and through the organisation
12. Robust challenge processes in place to ensure that the right information is being captured and presented to management
13. Clear criteria set for the escalation of risks
14. Easy access to practical guidance that is easy to understand
15. Focus is less on process and more creating the appropriate risk culture
16. Lessons are learned
17. Risk management is an enabler, helps managers to manage
18. Responding to risks considers the five T's (Treat. Tolerate, Transfer, Terminate, Take the opportunity)
19. Continuous improvement and refresh rather than keep doing the same things that don not work

Annex 3 – Management Response

Risk Management Audit Report 2008/09

Paper for the House of Commons Administration Audit Committee
from the Head of the Office of the Chief Executive (the Audit Sponsor))

Purpose of paper

1. This note gives the Audit Sponsor's preliminary response to the 2008/09 Internal Audit (IA) risk assurance audit report.

The main Audit Findings and CRMT responses

2. The Corporate Risk Management Team (CRMT) welcomes the 2008/09 risk management audit and fully accepts its findings. The team has already met with the audit sponsor and with the Internal Audit team (IA) to discuss these findings.

3. Many of the findings mirror feedback that the CRMT has received from stakeholders across the House Service.

4. The audit acknowledges the progress made in the House's risk management performance since the last full audit performed by PricewaterhouseCoopers, in 2007. In particular, it notes the considerable progress that has been made on improving **how** risk is managed across the House.

5. Notwithstanding these improvements, the audit identifies the need for a 'step-change' in risk management across the House.

6. Below are four main areas where the audit concludes that action is required, together with the CRMT's initial response.

    a. The House has in place a risk management policy statement and implementation strategy which follows best practice as recommended by the Treasury (Management of Risk – A Strategic Overview H M Treasury January 2004). The audit suggests that the Management Board review this policy to ensure it still remains appropriate for the organisation.
    The CRMT continues to believe that the existing 'risk embedded' model of risk management remains an appropriate model for the House of Commons (HoC). However, it will revisit the current policy of risk management with the Board to ensure that it retains confidence in the model.

    b. The CRMT has (to date) concentrated its resources on improving processes and procedures (ensuring risk registers are complete and up to date) at the expense of other areas of risk

management work which may add more value to the organisation.
The CRMT will now change the focus of its 'core' work and concentrate on working with managers to ensure that they are actively managing the corporate risks. This change of focus will involve a more 'challenging' role for the CRMT. The CRMT is determined to ensure that this change in focus will result in real and measurable benefits to managers in the House Service.

c. The audit report indicates that more work needs to be done to ensure that "*the organisation is open and transparent about those significant events that have an impact upon the assessment of the corporate risks":* at the same time the report explains that it is important to *"embed the CRMT in organisational reporting structures to ensure that they receive timely and detailed information on any events that relate directly to the top ten corporate risks and the management of those risks*" (both paragraph 7 IA).
The CRMT will work to promote risk management in a way that makes it 'real' for those people who are actively managing risk, and to ensure that they are aware of the benefits that good risk management can bring.

d. More work is also needed *"to improve the information in the departmental risk registers on mitigations*" (paragraph 11 IA); there is a concern that the underlying information that underpins corporate and departmental risk assessments may not be robust, leading to assessments being made on 'gut feelings'.
Significant work on this area has already started, the CRMT met with PricewaterhouseCoopers in April 2009, to look at improving the system of capturing the data supporting the mitigations.

7. A full response and action plan will be developed for the consideration of the Management Board in September 2009 and subject to the Board's approval reported to the Audit Committee in October 2009.

Philippa Helme
Office of the Chief Executive
July 2009