Audit Committee 21 June 2012

Internal audit report – Risk Management review

Executive summary and recommendations

Introduction

Mazars have undertaken a review of Risk Management, in accordance with the internal audit plan agreed by the committee in March 2011. The report is attached as an appendix to this paper.

The report rated this area "Substantial Assurance" and made 2 housekeeping recommendations.

Recommendation (6.1) concerning minutes of changes to Risk Registers at Executive Management Team meetings has already been agreed (as of February 2012).

Recommendation (6.2) concerning the inclusion of warning flags on the register to indicate the crystallisation of risks (as "*Risks not being clearly defined and understood*") seems disproportionate for an organisation of HPC's size. A mock-up of the warning flags monitoring report has been provided by Mazars "Warning signs for organisations" and this is attached.

Decision

The Committee is asked to discuss and approve the report.

Background information

Resource implications
None.

Financial implications
None.

Appendices
Internal Audit Report: Risk Management (05.11/12) May 2012
Warning signs for organisations May 2012

Date of paper
11 June 2012

Internal Audit Report

Risk Management (05.11/12)

May 2012

FINAL REPORT

CONTENTS

AUDIT CONTROL SCHEDULE:

Client contacts:	Greg Ross-Sampson: Director of Operations Roy Dunn: Head of Business Process Improvement Marc Seale: Chief Executive and Registrar	**Internal Audit Team:**	Peter Cudlip: Partner Graeme Clarke: Director Peter Williamson: Assistant Manager James Sherrett: Senior Auditor
Finish on Site \ Exit Meeting:	31 January 2012	**Management responses received:**	16 May 2012
Draft report issued:	13 February 2012	**Final report issued:**	22 May 2012

In the event of any questions arising from this report please contact Graeme Clarke, Director, Mazars LLP graeme.clarke@mazars.co.uk

Status of our reports

This report is confidential and has been prepared for the sole use of the Health Professions Council.

This report must not be disclosed to any third party or reproduced in whole or in part without the prior written consent of Mazars LLP. To the fullest extent permitted by law, no responsibility or liability is accepted by Mazars LLP to any third party who purports to use or rely, for any reason whatsoever, on this report, its contents or conclusions.

1. INTRODUCTION

1.1 As part of the Internal Audit Plan for 2011/12, we have undertaken a review of the Health Professions Council's (HPC) arrangements for risk management. This review is required in order to fulfil our professional obligations as Internal Auditors according to the requirements set by the Institute of Internal Auditors

1.2 We are grateful to the Director of Operations and the Head of Business Process Improvement for their assistance provided to us during the course of the audit.

1.3 This report is confidential and for the use of the Audit Committee and senior management of the Council. The report summarises the results of the internal audit work and, therefore, does not include all matters that came to our attention during the audit. Such matters have been discussed with the relevant staff.

2. BACKGROUND

2.1 HM Treasury guidance states that "Risk management covers all the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress. Good risk management helps reduce hazard, and builds confidence to innovate".

2.2 HPC's Audit Committee approved a statement in November 2010 defining the organisation's risk appetite as 'risk averse'. This sets the tone for the organisation's approach to risk management.

2.3 Risk management processes at HPC are embedded within the business planning cycle. For example, risks identified in the risk register include strategic risks which relate to HPC's Strategic Intentions and Directorate/Department risks which are aligned to the Annual Work Plans and objectives for those Directorates/ Departments. Significant projects undertaken by HPC also have their own risk registers as part of the usual project management processes. These Registers are also aligned and linked to the overall Risk Register.

2.4 Risk registers have a consistent format and clearly identify scoring, risk mitigation controls and responsibility for, and ownership of, risks and associated mitigation actions.

2.5 The Risk Register is subject to regular review and monitoring by senior management within HPC and formal review by all Risk Owners and the Executive Management Team (EMT) on a six-monthly basis. The Audit Committee also receives assurances on the adequacy and effectiveness of risk management arrangements on a regular basis through a variety of means. These include formal presentations by Risk Owners, on a rotation basis, to the Audit Committee covering the risks for which they are responsible. The Audit Committee also receives a 'Top Ten Risks' paper at six monthly intervals.

2.6 On our appointment as internal auditors to HPC and through attendance at each meeting of the Audit Committee, we are aware of a longstanding point of discussion between members of the Audit Committee and EMT on the content and format of the Risk Register. EMT have made changes to the Risk Register in response to this and the Audit Committee confirmed it was happy with the approach taken at its meeting in March 2012.

3. SCOPE AND OBJECTIVES OF THE AUDIT

3.1 Our audit considered the following risks relating to the area under review:

- Employees do not know what they are responsible for, or how to carry out their duties, leading to failure to follow the Risk Management Strategy and related procedures;
- New and emerging risks are not identified or acted on/escalated in a timely and efficient manner;
- Weak or non-existent controls to mitigate against the risks associated with HPC's objectives, leading to non-achievement of objectives, financial loss or adverse PR; and
- Failure to review/monitor risks in a regular structured manner, leading to non-achievement of HPC's objectives.

3.2 In reviewing the above risks, our audit considered the following areas:

- Risk Management Strategy and Policy;
- Risk Register;
- Documentation of Risk Management roles and responsibilities;
- Administration and maintenance of HPC's Risk Register including its review and update during the year;
- Pro-forma for recording newly identified risk;
- Processes for the identification, scoring and recording of risk;
- Communication of the Strategy and Policy;
- Training on the Risk Management framework for New and existing Risk Owners; and
- Audit trail of discussion of risk management at EMT Risk Management Group/Audit Committee and Council Meetings.

3.3 The objectives of our audit were to evaluate the adequacy and effectiveness of HPC's arrangements for risk management, and the extent to which controls have been applied, with a view to providing an opinion on the extent to which risks in this area are managed. In giving this assessment, it should be noted that assurance cannot be absolute. The most an Internal Audit service can provide is reasonable assurance that there are no major weaknesses in the framework of internal control.

3.4 We are only able to provide an overall assessment on those arrangements for risk management that we have tested or reviewed. The responsibility for maintaining internal control rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy of the internal control arrangements implemented by management and perform testing on those controls to ensure that they are operating for the period under review. We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone are not a guarantee that fraud, where existing, will be discovered.

4. AUDIT FINDINGS: ONE PAGE SUMMARY

Assurance on effectiveness of internal controls	
🟢	**Substantial Assurance**

Recommendations summary	
Priority	**No. of recommendations**
1 (Fundamental)	None
2 (Significant)	None
3 (Housekeeping)	2
Total	**2**

Risk management

HPC has a clearly stated risk appetite which has been approved by the Audit Committee. This sets the tone for the approach to risk management throughout the organisation. Risk management processes at HPC are embedded within the business planning cycle. Directorate and Department Annual Work Plans identify objectives, which are aligned to the objectives for HPC as a whole as stated in the Strategic Intentions document. Risk management arrangements are incorporated into these Work Plans.

The Risk Register is subject to formal review by the Chief Executive and Registrar, Director of Operations and Head of Business Process Improvement on a regular basis and by the whole Executive Management Team on a six-monthly basis enabling a co-ordinated approach across HPC. Responsibility for, and ownership of, risks and associated mitigation actions are clearly documented in the Risk Register.

Risk management at HPC is monitored and reviewed throughout the organisation including Executive Management Team, Audit Committee and Council level.

Value for money

HPC’s risk management processes and arrangements appear to be streamlined and co-ordinated in an effective and efficient manner. This includes reporting by Risk Owners to the Audit Committee on their areas of responsibility and the use of a ‘Top Ten Risks’ paper.

5. SUMMARY OF FINDINGS

Overall conclusion on effectiveness and application of internal controls

5.1 Taking account of the issues identified in paragraphs 5.2 and 5.3 below, in our opinion HPC's arrangements for risk management, as currently laid down and operated at the time of our review, provides **substantial** assurance that risks material to the achievement of HPC's objectives for this area are adequately managed and controlled.

Areas where controls are operating effectively

5.2 The following are examples of controls which we have considered are operating effectively at the time of our review:

- HPC has a clearly stated risk appetite which has been approved by the Audit Committee;
- The Risk Register is subject to formal review by the Chief Executive and Registrar, Director of Operations and Head of Business Process Improvement on a regular basis and by the whole Executive Management Team on a six-monthly basis;
- A clear risk scoring methodology is used on a consistent basis for both strategic risks faced by HPC and for risks faced by Directorates and Departments;
- Responsibility for, and ownership of, risks and associated mitigation actions are clearly documented in the Risk Register;
- Risk management processes are embedded within the business planning cycle and Directorate and Department Annual Work Plans recognise potential risks to the achievement of objectives and identify risk mitigation controls and arrangements;
- Significant projects undertaken by HPC, such as taking over the responsibilities of the General Social Care Council (GSCC), have their own risk registers as part of the usual project management processes. The format and scoring methodologies for these risk registers is consistent with the overall HPC risk register. Project Risk Registers are aligned and linked to the overall Risk Register;
- The Audit Committee receives a 'Top Ten Risks' paper at six monthly intervals; and,
- On a rotation basis, Risk Owners are required to present the risks to the Audit Committee for which they are responsible.

Areas for further improvement

5.3 We identified certain areas where there is scope for further improvement in the control environment. The matters arising have been discussed with management, to whom we have made a number of recommendations. The recommendations have been, or are being, addressed as detailed in the management action plan (Section 6 below).

6. ACTION PLAN

Risk 2: New and emerging risks are not identified or acted on / escalated in a timely and efficient manner.

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
6.1	*Observation:* The Risk Register is presented, discussed and reviewed every six months at Executive Management Team (EMT) meetings, prior to the register being presented to the Audit Committee meeting. The risk register is agreed by the full EMT at this stage. Review of the minutes of EMT meetings confirmed that any changes to risks scoring and/or any new risks being added are clearly recorded. However, there could be more detail provided as to the justification for any such amendments. *Risk:* Decision-making in relation to changes to risk scores, mitigation arrangements and/or the identification of new risks is not clearly recorded.	Consideration should be given to greater detail in EMT minutes recording the justification for amendments to the Risk Register.	3	The EMT will include in the minutes reasons for changes to the risk register.	Implemented February 2012 by the Chief Executive & Registrar

Risk 3: Weak or non-existent controls to mitigate against the risks associated with HPC's objectives, leading to non-achievement of objectives, financial loss or adverse PR.

	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
6.2	*Observation:* The HPC risk register groups risks under Strategic Risks and risks which are grouped so as to align to Directorates or Departments as identified within respective Annual Work. Descriptions of risks are brief and there is no description or identification of indicators/warning signs that risks may be crystallising other than through the formal review process of the Register itself by the EMT. *Risk:* Risks are not clearly defined and understood and early indicators that risk may be materialising are not recognised.	Consideration should be given to identifying 'early warning signals' on the Risk Register, against significant risks, which would 'flag-up' the types of events/occurrences which indicate that the risk is likely to crystallise.	3	The EMT would like to examine working examples of such early warning flagging mechanisms, to determine if they are appropriate and workable at HPC. We would like Mazars to provide examples from similar sized organisations working in similar areas if possible. *Audit Comment* We have provided an illustrative example of the types of early warning indicators used in other organisations for consideration.	

Appendix 1 – Definitions of Assurance Levels and Recommendations

We use the following levels of assurance and recommendations in our audit reports:

Assurance Level	Adequacy of system design	Effectiveness of operating controls
Substantial Assurance:	While a basically sound system of control exists, there is some scope for improvement.	While controls are generally operating effectively, there is some scope for improvement.
Adequate Assurance:	While a generally sound system of control exists, there are weaknesses which put some of the system objectives at risk.	While controls are generally operating effectively, there are weaknesses which put some of the system objectives at risk.
Limited Assurance:	Control is generally weak leaving the system open to significant error or abuse.	Control is generally weak leaving the system open to significant error or abuse.

Recommendation Grading	Definition
Priority 1 (Fundamental)	Recommendations represent fundamental control weaknesses, which expose, HPC to a high degree of unnecessary risk.
Priority 2 (Significant)	Recommendations represent significant control weaknesses which expose, HPC to a moderate degree of unnecessary risk.
Priority 3 (Housekeeping)	Recommendations show areas where we have highlighted opportunities to implement a good or better practice, to improve efficiency or further reduce exposure to risk.

Warning signs for organisations

May 2012

Risk	Description	Early warning indicators	Mitigation	Ranking (Red / Amber / Green)
Financial loss	Corporate memory loss as staff leave. Expertise lost, rework and loss of negotiating position.	Departure of two or more directors / deputies or from same directorate. NED vacancies / roles not covered.	Up to date policy and procedure manuals. Assurance Framework	
Performance	Staff performance drops as attention diverted to changes / personal futures / motivation.	Slippage on major deliverables.	Advance change management processes.	
Control	Multiple agendas (savings,. moves, etc) increase workloads. Risk increases as people try to absorb additional workloads within existing resource and do not recognise deteriorating position / increased risk profile – "frog in boiling water". Policies get out of date or in conflict following mergers.	Slippage on major deliverables. Financial position worsens. Long hours culture, holiday sacrifice by senior managers.	Prioritise outputs rather than do everything. Audit Committee scrutiny internal / external audit. Assurance Framework	

Risk	Description	Early warning indicators	Mitigation	Ranking (Red / Amber / Green)
Performance / financial	Strain of delivering diverse change agendas allows gaps / exposes weaknesses; paradigm shift (attitudinal change); organisational change (closing down / creating new organisations); business as usual; savings targets.	Slippage on major deliverables. Under-developed changes implemented.	Audit Committee Internal audit	
Financial loss	Costs of change (redundancies and process) exceed financial reserves.	Redundancy notices issued without evaluation assessments.	Establish thorough evaluation process and project management.	
Financial and quality	Risk management reduced as an impact of immediate pressure.	Risk management slips off agendas. Increased number of adverse 'incidents'.	Meeting chairs retain focus on risk management.	
Reputation	Perceive reduced service access	Media reports, complaints, referral levels to appeal panels.	Proactive local media communication on service changes. Advanced briefings.	

Risk	Description	Early warning indicators	Mitigation	Ranking (Red / Amber / Green)
Performance	Reduced capacity as staff are diverted by HR change process and / or leave	Slippage on major deliverables.	Retention strategies for key staff.	
Performance and financial	Staff performance drops as a result of demotivation.	Sickness rates rise. Key staff leave.	Communication.	