Audit Committee 5 September 2017

Risk Assurance mapping at HCPC

Executive summary and recommendations

Introduction

In the Audit Committee of March 2017 the executive were asked to provide examples of the risk assurance mapping for sample parts of the risk register. In Audit Committee of June 2017, the Audit Committee Chair indicated changes to the areas of assurance should be discussed. Education & Training Committee and Remuneration Committee have subsequently been proposed as being included in the Area A assurance.

Increasing Assurance →

AREA C. Management Control & Reporting				**AREA B**. Functional oversight / Governance	**AREA A**. Independent review / Assurance / Regulatory oversight												
Systems Controls	Operational Risk Management	Inter-departmental Quality Assurance	Near Miss Reporting	EMT	Council	Audit Comm	ETC	Rem Comm	Internal Auditors	External Auditors (NAO)	External Legal Advice	Quality Management System ISO9001	Information Security Management ISO27001	PSA	Penetration Testing	PCI-DSS	Parliamentary oversight

The proposed new assurance providers in Area A are indicated in the red columns. The grid above would be applied to all sections of the risk register at a later date.

Changes to Audit Committee areas of assurance are indicated in the table attached as follows; 0 indicates removal of assurance (also in red), PSA assurance around Partners has also been removed.

The Chair of Council has proposed gaps created by the removal from Audit Committee be covered by other committees as indicated. Proposed additions are indicated with a red X'. Other minor changes are also indicated.

Decision

Committee is asked to discuss the proposal, or suggest another approach if required.

Background information

Risk Assurance mapping has been in place since 2015.

Assurance will be grouped as indicated below;

AREA C. Management Control & Reporting
Team Leader, Department Managers, Heads of, analysis of performance and trends within departments; departmental Quality Assurance processes, internal Near Miss Reporting for events with the potential for reputation damage.

AREA B. Functional oversight / Governance

Oversight of functions by line manager EMT members, Chief Executive & Registrar, and fellow EMT members. (includes monitoring of monthly reporting outputs).

AREA A. Independent review / Assurance / Regulatory oversight

Includes all external audit functions focused on HCPC, BSI (ISO9001 & ISO27001 audit process and schedule), Professional Standards Authority (PSA performance review), Contracted Internal Auditors (PKF, Mazars, Grant Thornton etc), External Auditors (National Audit Office, Baker Tilly). Council and Audit Committee would now be joined by Education & Training Committee and Remuneration Committee.

Assurance is considered when new risks are added or significantly changed. Assurance is considered when the risk register is updated, however changes in assurance are infrequent.

Organisations aim to provide “Reasonable Assurance” that their risk responses are appropriate. However, all audit activity is a burden on an organisations resources, and one must consider the impact and the potential benefit to the organisation and its stakeholders.

As HCPC has a low risk appetite and catastrophic scenarios are highly unlikely to occur, excessive audit of assurance mechanisms are unlikely to be cost effective.

Resource implications

The Executive will determine any resource implications following the decision from this paper.

Financial implications

None

Date of paper

29th August 2017

HCPC Risk Assurance mapping

Increasing Assurance

Proposed	AREA C. Management Control & Reporting				AREA B. Functional oversight / Governance	AREA A. Independent review / Assurance / Regulatory oversight												
Key Business Risk areas Assurance Map	**Systems Controls**	**Operational Risk Management**	**Inter-departmental Quality Assurance**	**Near Miss Reporting**	**EMT**	**Council**	**Audit Comm**	**ETC**	**Rem Comm**	**Internal Auditors**	**External Auditors (NAO)**	**External Legal Advice**	**Quality Management System ISO9001**	**Information Security Management ISO27001**	**PSA**	**Penetration Testing**	**PCI-DSS**	**Parliamentary oversight**
Strategic risks						x				x		x						x
Communications		x	x	x	x	x	0			x	x	x	x		x			
Continuing Professional Development	x	x	x	x	x		0	X'				x						
Corporate Governance			x	x	x	x	x	x'		x	x	x	x		x			x
Information Security	x	x	x	x	x		x			x			x	x		x	x	
Education	x	x	x	x	x	x	0	X'		x		x	x		x			
Finance	x	x	x	x	x	x	x			x	x	x	x	x			x	x
Fitness to Practise	x	x	x	x	x	x	0			x		x	x	X'	x			x
HR	x	x	x	x	x	x	0		X'	x		x	x	x				
Information Technology	x	x	x	x	x	x	x			x	x	x	x	x		x	X'	
Legal				x	x	x	0			x		x			x			x
Operations	x	x	x	x	x	x	x			x	x		x		x			
Partner	x	x	x	x	x	x	0			x			x	x	0			
Pensions				x	x	x	0		X'	x		x						
Policy & Standards			x	x	x	x	0			x		x	x		x			x
Project Management	x	x	x	x	x	x	X			x	x		x	x				
Quality Management	x	x	x	x	x	x	x			x			x		x			
Registration	x	x	x	x	x	x	x			x		x	x		x			

Add ETC = Corporate Governance

Add ISO27001 = FTP

Add Rem Comm = HR

Add PCI-DSS = Information Technology

Remove PSA = Partners

Add Rem Comm = Pensions

Add Audit Comm = Proj Mgmt

HCPC Risk Assurance mapping

Increasing Assurance

Current	AREA C. Management Control & Reporting				AREA B. Functional oversight / Governance	AREA A. Independent review / Assurance / Regulatory oversight										
Key Business Risk areas Assurance Map	**Systems Controls**	**Operational Risk Management**	**Inter-departmental Quality Assurance**	**Near Miss Reporting**	**EMT**	**Council**	**Audit Committee**	**Internal Auditors**	**External Auditors (NAO)**	**External Legal Advice**	**Quality Management System ISO9001**	**Information Security Management ISO27001**	**PSA**	**Penetration Testing**	**PCI-DSS**	**Parliamentary oversight**
Strategic risks						x	x	x		x						x
Communications		x	x	x	x	x	x	x	x	x	x		x			
Continuing Professional Development	x	x	x	x	x		x			x						
Corporate Governance			x	x	x	x	x	x	x	x	x		x			x
Information Security	x	x	x	x	x		x	x			x	x		x	x	
Education	x	x	x	x	x	x	x	x		x	x		x			
Finance	x	x	x	x	x	x	x	x	x	x	x	x			x	x
Fitness to Practise	x	x	x	x	x	x	x	x		x	x		x			x
HR	x	x	x	x	x	x	x	x		x	x	x				
Information Technology	x	x	x	x	x	x	x	x	x	x	x			x		
Legal				x	x	x	x	x		x			x			x
Operations	x	x	x	x	x	x	x	x	x		x		x			
Partner	x	x	x	x	x	x	x	x			x	x	x			
Pensions				x	x	x	x	x		x						
Policy & Standards			x	x	x	x	x	x		x	x		x			x
Project Management	x	x	x	x	x	x	x	x	x		x	x				
Quality Management	x	x	x	x	x	x	x	x			x		x			
Registration	x	x	x	x	x	x	x	x		x	x		x			