hcpc | health & care professions council

Audit Committee 26 November 2015

Risk Assurance mapping at HCPC

Executive summary and recommendations

Introduction

At the Audit Committee of 8 September 2015, the Executive were asked to provide examples of the risk assurance mapping for sample parts of the risk register.

The Risk register has been in place since 2003, and has undergone many improvements to ensure it is fit for purpose. The current format of HCPC's risk register has been in place since 2009.

In 2014 a section was added to the end of the risk register to illustrate overall risk assurance around HCPC for each of the major groups of risks. Three major categories of assurance are indicated.

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)

										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 Committee	Internal Auditors	External Auditors (NAO)	External Legal Advice	Quality Management System ISO9001	Information Security Management ISO27001	PSA	Penetration Testing	PCI-DSS	Parliamentary or government oversight	Assurance Status Flag; Good, Medium, Poor

The grid above has been applied to all sections of the risk register.

This broad approach to Risk Assurance was applied to all risks, by the risk owners. The assurance mapping makes the risk register more difficult to read whilst not adding additional assurance to the committee. This will become apparent when we examine the assurance mapping for the following key risk areas;

- o Human Resources Risks
- o Fitness to Practise Risks

        o Strategic Risks

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 the 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.

There is little to gain from an increased risk appetite at a regulator of health and care professionals, so the level of assurance in our environment is unlikely to change in the short to medium term.

Decision

Committee is asked to discuss the report and associated examples of risk assurance and provide direction to the Executive as to whether this level of risk assurance mapping is fit for purpose, or if another approach is required.

Background information

HCPC's Risk Appetite statement

> The HCPC is a UK statutory regulator of Health and Care professionals, with the objective of protecting the public.

> HCPC has an **averse** appetite to risk in that we;

> 1. Identify all relevant risks
> 2. Mitigate those risks to an appropriate level
> 3. Invest mitigation resources in proportion to the level of risk

Resource implications

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

Financial implications

None

Appendices

Date of paper

16 November 2015

DOCUMENT CONTROL: Reference Risk Treatment Plan. Version Aug 2015 Version 1.0
Issue Date: 01/09/2015 Classification: Public

RISK ASSESSMENT &

Risk Register & Risk Treatment Plan - Assurance demonstration

Marc Seale, Chief Executive & Registrar
Report to Audit Committee, (Aug 2015)

Latest version stored on Intranet in Quality Management System \ Quality \ Risk Management

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

Strategic

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 Committee	Internal Auditors	External Auditors (NAO)	External Legal Advice	Quality Management System ISO9001	Information Security Management ISO27001	PSA	Penetration Testing	PCI-DSS	Parliamentary or government oversight	Assurance Status Flag; Good, Medium, Poor	Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
					X	X	X		X			X			X	G	1	Strategic		1.1	HCPC fails to deliver SI Sec 6.2 & Health Bill	Council	5	1	5	Delivery of HCPC Strategy	Publication of Annual Report	Ensure Strategic Intent is up to date	Low	Low
																					Links to 7.1-7.4, 8.1-8.2, 10.4, 10.5, 11.4, 15.9									
					X				X							G		Strategic		1.2	Unexpected change in UK legislation	Chief Executive	5	2	10	Relationship with Government depts	Enviromental scanning	-	Low	Low
																					Links to 2.2,									
					X	X	X		X							G		Strategic	I	1.3	Incompatible SI Sec 6.2 & Health Bill and EU legislation	Chief Executive	1	3	3	Monitoring of EU directives e.g. Professional Qualifications Directive	Membership of Alliance of UK Health Regulators on Europe (lobby group)	-	Low	Low
					X											G		Strategic		1.4	Failure to maintain a relationship with PSA	Chief Executive & Chair	5	1	5	HCPC Chair and Chief Executive relationship with PSA	Communications	-	Low	Low
				X	X										X	G		Strategic	I	1.5	Loss of reputation	Chief Executive & Chair	5	3	15	Quality of governance procedures	Quality of operational procedures	Dynamism and quality of Comms strategy	Medium	Medium
					X	X	X		X							G		Strategic		1.6	Failure to abide by current Equality & Diversity legislation	Chief Executive	4	2	8	Equality & Diversity scheme	Implimentation of scheme for employees Implimentation of scheme for partners	Equality & Diversity working group	Low	Low
				X												G		Strategic		1.7	Failure to maintain HCPC culture	Chief Executive	5	2	10	Behaviour of all employees	Induction of new employees	Internal communication	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

HR

→ 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 Committee	Internal Auditors	External Auditors (NAO)	External Legal Advice	Quality Management System ISO9001	Information Security Management ISO27001	PSA	Penetration Testing	PCI-DSS	Parliamentary or government oversight	Assurance Status Flag; Good, Medium, Poor.	Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
X	X			X		X				X						G	11	HR		11.1	Loss of key HCPC employees	Chair, Chief Executive and EMT	3	2	6	Organisation succession plan held by Chief Executive and HR Director.	Departmental training (partial or full) and process documentation	Informal department level succession plans	Low	Low
X				X	X	X	X			X						G		HR		11.2	High turnover of employees	HR Director	3	3	9	Remuneration and HR strategy	Regular performance reviews	Exit interview analysis and employee survey analysis	Low	Low
																					Links to 11.3									
	X			X												G		HR		11.3	Inability to recruit suitable employees	HR Director	3	3	9	Recruitment strategy and adequate resourcing of the HR dept	Careful specification of recruitment adverts and interview panel selection	Hire skilled temporary employees in the interim	Low	Low
																					Links to 4.10, 6.1, 11.2, 11.8									
X	X		X	X	X	X	X	X		X						G		HR		11.4	Lack of technical and managerial skills to delivery the HCPC strategy	Chief Executive	4	2	8	HR strategy and Performance and Development management: -Buy in skills -Upskilling employees on the job -Training	Training needs analysis & training delivery including Management Development Programme	Some projects or work initiatives delayed or outsourced	Low	Low
																					Links to 1.1									
X	X			X		X										G		HR		11.6	High sick leave levels	EMT	2	2	4	Adequate employees (volume and type) including hiring temporary employees	Return to work interviews and sick leave monitoring	Regular progess reviews	Low	Low
	X			X		X	X		X							G		HR		11.7	Employee and ex-employee litigation	HR Director	4	3	12	Regular one to one sessions between manager and employee and regular performance reviews.	Keeping HR policies and processes in line with employment legislation	Employee surveys, Exit interviews, Employee Assistance Programme, Management Development Programme.	Low	Low
X	X			X					X							G		HR	I	11.8	Employer/employee inappropriate behaviour	HR Director	2	2	4	Whistle blowing policy, Code of Conduct & Behaviour	Other HR policies and procedures	Employee Assistance programme	Low	Low
																					Links to 11.3									
X	X			X					X							G		HR		11.9	Non-compliance with Employment legislation	HR Director	4	2	8	Up to date HR policies and processes in line with employment legislation.	Obtain legislation updates and legal advice	HR training for managers	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

Fitness to Practise

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 Committee	Internal Auditors	External Auditors (NAO)	External Legal Advice	External Legal Advice	Quality Management System ISO9001	Information Security Management ISO27001	PSA	Penetration Testing	PCI-DSS	Parliamentary or government oversight	Assurance Status Flag: Good, Medium, Poor.	Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---
X	X			X		X	X	X									G	13	Fitness to Practise		13.1	Legal cost over-runs	FTP Director	4	4	16	Contractual and SLA arrangements with legal services providers(s)	Quality of operational procedures	Quality assurance mechanisms	Low	Low
																						Links to 13.4, 15.2									
X	X			X		X	X	X									G		Fitness to Practise		13.3	Tribunal exceptional costs	FTP Director	5	5	25	Quality of operational processes	Accurate and realistic forecasting	Quality of legal advice	Medium	Medium
																	G		Fitness to Practise		13.4	Rapid increase in the number of allegations and resultant legal costs	FTP Director	4	4	16	Accurate and realistic budgeting	Resource planning	-	Medium	Medium
																						Links to 13.1									
X	X			X					X			X					G		Fitness to Practise		13.5	Witness non-attendance	FTP Director	4	2	8	Vulnerable witness provisions in the legislation	Witness support programme	Witness summons	Low	Low
X	X		X	X		X											G		Fitness to Practise	I	13.6	Employee/Partner physical assault by Hearing attendees	FTP Director	5	5	25	Risk Assessment Processes	Adequate facilities security	Periodic use of security contractors and other steps	Low	Low
X	X			X								X			X		G		Fitness to Practise		13.7	High Number of Registration Appeals	FTP Director & Director of Operations, Head of Registrations	3	5	15	Training and selection of Registration Assessors, so reasoned decisions are generated	Quality of operational processes	-	Low	Low
X	X			X	X	X	X			X		X			X		G		Fitness to Practise		13.8	Backlog of FTP cases	FTP Director	3	4	12	Reforecasting budget processes	Monthly management reporting	Quality of operational processes	Low	Low
X	X			X		X	X			X							G		Fitness to Practise		13.9	Excessive cases per Case Manager workload	FTP Director	3	4	12	Reforecasting budget processes	Monthly management reporting	Resource planning & Quality of operational processes	Low	Low
																						13.2 moved to 12.2									
											X						G		Fitness to Practise	I	13.10	Protracted service outage following a Case Management System failure	Director of IT	5	3	15	Effective backup and recovery procedures	Maintenance and support contracts for core system elements	Annual IT continuity tests	Low	Low

HCPC Risk Assurance mapping

Increasing Assurance

Key Business Risk areas Assurance Map	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 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		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			