Audit Committee, 14 June 2017

Risk Assurance mapping at HCPC

Executive summary and recommendations

Introduction

At 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. Operations and Corporate Governance have been selected for the demonstration. These are presented in the attachment.

The Risk register has been in place since 2003, and has had many improvements to ensure it is fit for purpose. The current format of HCPC's risk register has been in place since 2009, with Risk Assurance mapping added in 2015.

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 so other than for demonstration purposes, or when Audit Committee requests detail the assurance maps for all risks are not published. This will become apparent when we examine the assurance mapping for the following key risk areas;

- Operations Risks
- Corporate Governance Risks

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.

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

None

Resource implications

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

Financial implications

None

Date of paper

23 May 2017

Risk Register & Risk Treatment Plan

Marc Seale, Chief Executive & Registrar
Report to Council, (April 2017)

Risk Assurance Mapping demonstration

hcpc health & care professions council

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN Apr 2017

Operations

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 C/I/A indicates attributes considered	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Apr 2017	Likelihood before mitigations Apr 2017	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Apr 2017	RISK score after Mitigation Jan 2017
	X		X	X		X	X			X						G	2	Operations	I A11, 17.2.1 x/I/A TRT>TOL	2.1	Inability to occupy premises or use interior equipment	Office Services Mgr	4	4	16	Invoke Disaster Recovery/Business Continuity plan	Commercial combined insurance cover (fire, contents, terrorism etc)	-	Low	Low
X	X			X		X				X						G		Operations		2.2	Rapid increase in registrant numbers	Chief Executive and EMT	3	4	12	Scaleable business processes and scalable IT systems to support them	Influence the rate at which new professions are regulated	-	Low	Low
																					Links to 1.2, 13.4								
X	X	X	X	X			X		X	X					X	G		Operations		2.3	Unacceptable service standards	Director of Operations	5	4	20	ISO 9001 Registration, process maps, well documented procedures & BSI audits	Hire temporary employees to clear service backlogs	Detailed workforce plan to match workload.	Low	Low
																					Links to 9.1, 10.4								
			X	X						X						G		Operations		2.4	Inability to communicate via postal services (e.g. Postal strikes)	Office Services Mgr	3	3	9	Use of other media including Website, newsletter & email and courier services	Invoke Business Continuity Plan	Collection of >80% income fees by DD	Medium	Medium
	X		X	X	X	X	X			X	X					G		Operations		2.5	Public transport disruption leading to inability to use Park House	Office Services Mgr & Head Bus Proc	4	5	20	Contact employees via Business Continuity Plan process	Make arrangements for employees to work at home if possible	-	Low	Low
	X		X	X						X						G		Operations	I A11 x/I/A TRT>TOL	2.6	Inability to accommodate HCPC employees	Office Services Mgr	4	3	12	Ongoing Space planning	Additional premises purchase or rented	-	Low	Low
																					Links to 5.2								
				X						X						G		Operations	I A11.2.2 C/I/A TRT>TOL	2.7	Interruption to electricity supply	Office Services Mgr	4	4	16	Relocate to other buildings on site	If site wide longer than 24 hours invoke BCM/DR Plan	-	High	High
			X	X						X						G		Operations		2.8	Interruption to gas supply	Office Services Mgr	1	2	2	Temporary heaters to impacted areas	-	-	Low	Low
				X						X						G		Operations		2.9	Interruption to water supply	Office Services Mgr	2	2	4	Reduce consumption	Temporarily reduce headcount to align with legislation	Invoke DR plan if over 24 hrs	Low	Low
			X	X			X			X	X					G		Operations		2.10	Telephone system failure causing protracted service outage	Director of IT	4	3	12	Support and maintenance contract for hardware and software of the ACD and PABX	Backup of the configuration for both the ACD and PABX	Diverse routing for the physical data lines, Redundant exchange configuration, Dynamic capacity increases.	Low	Low
	X		X	X		X				X						G		Operations	I A11, 17 x/I/A TRT>TOL	2.11	Basement flooding	Office Services Mgr	4	4	16	Flood barrier protection to prevent ingress	Periodic descaling of drainage		Medium	Medium
	X			X		X	X			X	X					G		Operations		2.12	Significant disruption to UK transport network by environmental extremes e.g . snow, rain, ash; civil unrest or industrial action; disrupts planned external activities	Director of Operations & Head Bus Proc	3	2	6	Use of alternate networks	Use of video or teleconferencing facility to achieve corum	Invoke Disaster Recovery/Business Continuity plan	Low	Low
				X	X	X	X			X						G		Operations		2.14 (formerly11.5)	Health & Safety of employees	Chief Executive & Office Services Mgr	5	4	20	Health & Safety Training, policies and procedures	H&S Assessments	Personal Injury & Travel insurance	Low	Low
																					Links to 4.9, 6.3								
X		X		X		X	X									G		Operations		2.15	Expenses abuse by Partners not prevented	Director of FTP, Director of Education, Head of Registration, Partner Manager	1	2	2	Clear and appropriate Partner Expenses policy	Sign off by "user" departments	Planned travel supplier only policy in near future	Low	Low
			X	X						X	X					M		Operations	NEW	2.16	Loss of access to HCPC premises due to tunnel engineering failure (Northern Line Extension)	Director of Operations & Head Bus Proc, Office Services Mgr	5	2	10	Invoke Disaster Recovery/Business Continuity plan			Low	NEW
X	X		X	X						X	X					G		Operations	NEW	2.17	Damage or requirement for evacuation of operational premises due to rebuild/refurbishment activity of 186 KPR	Director of Operations & Head Bus Proc, Office Services Mgr	4	2	8	Building programme surveying and planning	Temporary changes to use of 184 KPR	Business Continuity plan	Low	NEW

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN Apr 2017

Corporate Governance

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 ISOZ7001**	**PSA**	**Penetration Testing**	**PCI-DSS**	**Parliamentary or government oversight**	**Assurance Status Flag; Good, Medium, Poor.**	**Ref**	**Category**	**ISMS Risks C/I/A indicates attributes considered**	**Ref #**	**Description**	**Risk owner (primary person responsible for assessing and managing the ongoing risk)**	**Impact before mitigations Apr 2017**	**Likelihood before mitigations Apr 2017**	**Risk Score = Impact x Likelihood**	**Mitigation I**	**Mitigation II**	**Mitigation III**	**RISK score after Mitigation Apr 2017**	**RISK score after Mitigation Jan 2017**
					X				X						X	G	4	Corporate Governance		4.1	Council inability to make decisions	Director of Council & Committee Services, & Chair	3	1	3	Regular meetings, agendas and clear lines of accountability between Council and committees	Well researched and drafted decision papers at meetings	Robust and effective recruitment process	Low	Low
																					Links to 4.4								
					X	X			X							G		Corporate Governance		4.2	Council members conflict of interest	Chair	4	3	12	Disclosure of members' interests to the Secretariat and ongoing Council & committee agenda item	Annual reminder to update Register of Interests	Member induction and training	Low	Low
					X	X		X	X						X	G		Corporate Governance		4.3	Poor Council decision-making due to conflicting advice or decision process	Chair	4	1	4	Well-researched & drafted decision papers, Clear lines of accountability and scheme of delegation	Chair facilitates well reasoned decisions	Attendance by external professionals, as required.	Low	Low
					X	X	X					X				G		Corporate Governance		4.4	Failure to meet Council/Committee quorums / failure to make quorate decisions	Director of Council & Committee Services	4	3	12	Clear communication of expectations of Council members' duties upfront	Adequate processes notifying Council & committee members of forthcoming meetings prior to meeting icluding confirmation of attendance	Robust discussions at annual appraisal	Low	Low
																					Links to 4.1								
					X	X										G		Corporate Governance		4.5	Members' poor performance	Chair	4	1	4	Appointment against competencies	Annual appraisal of Council members	Removal under Sch 1, Para 9(1)(f) of the HSWPO 2001	Low	Low
					X	X						X			X	G		Corporate Governance		4.6	Poor performance by the Chair	Council	5	1	5	Appointment against competencies	Power to remove the Chair under Sch 1, Article 12(1) C of the HSWPO 2001	External appraisal and effective feedback from fellow Council members	Low	Low
					X	X						X			X	G		Corporate Governance		4.7	Poor performance by Chief Executive	Chair	5	1	5	Performance reviews and regular "one to ones" with the Chair	Contract of Employment	-	Low	Low
						X	X	X								G		Corporate Governance		4.8	Improper financial incentives offered to Council members/employees	Chair and Chief Executive	4	2	8	Gifts & Inducements policy	Council member code of conduct	Induction training re:adherence to Nolan principles & Bribery Act 2010	Low	Low
				X	X	X	X	X	X	X						G		Corporate Governance		4.9	Failure to ensure the Health & Safety of Council Members ? Should this be HCPC wide?	Director of Council & Committee Services , Office Services Mgr & Finance Director	4	2	8	Safety briefing at start of each Council or Committee meeting.	H&S information on Council iPads	Personal Injury and Travel insurance	Low	Low
																					Links to 6.3								
					X	X	X	X	X			X			X	G		Corporate Governance		4.10	Establishing appropriately constituted Council	Chair	4	2	8	Robust and effective recruitment process	Use of skills matrix in recruitment exercise	Induction of Council members	Low	Low
																					Links to 6.1, 11.13								
	X			X		X	X	X								G		Corporate Governance		4.11	Expense claim abuse by members	Director of Council & Committee Services	4	2	8	Members Code of Conduct (public office)	Clear and comprehensive Council agreed policies posted on the Council member ipads and made clear during induction	Budget holder review and authorisation procedures	Low	Low
X	X			X	X	X	X	X	X	X					X	G		Corporate Governance		4.12	To ensure Section 60 legislation is operationalised effectively	Council	5	2	10	Scheme of delegation	Council Reporting	Quality Management Processes (ISO9001)	Low	Low
X	X								X	X		X			X	G		Corporate Governance		4.13	Failure to comply with DPA 1998 or FOIA 2000, leading to ICO action	Director of Council & Committee Services	3	3	9	Legal advice	Clear ISO processes	Organisation-wide training	Low	Low
				X		X	X	X	X							G		Corporate Governance	I A18.1.1 x/I/A TRT>TOL	4.15	Failure to adhere to the requirements of the Bribery Act 2010	Chair, & Director of Council & Committee Services	4	2	8	Suite of policies and processes related to the Bribery Act	Quality Management Systems	Oversight of EMT, Internal Audit & External Audit	Low	Low
					X	X										G		Corporate Governance		4.16	PSA fails to recommend appointment of Council members to the Privy Council	Director of Council & Committee Services	1	5	5	Sign off of high level process by Council	PSA comments on advance notice of intent acted on appropriately	Effective engagement with PSA throughout process	Low	Low
					X	X	X	X	X			X			X	G		Corporate Governance		4.17	Failure to meet requirements of the constitution order	Director of Council & Committee Services	3	1	3	Scrutiny of advance notice of intent	Targeted advertising strategy	_	Low	Low

Appendix i

Glossary & Abbreviations

Term	Meaning
AGM	Annual General Meeting
BCP / BCM	Business Continuity Plan / Business Continuity Management (Disaster Recovery and associated processes)
CCM's	Council & Committee Members
CDT	Cross Directorate Team (formerly HCPC's Middle Management Group)
CPD	Continuing Professional Development
EEA	European Economic Area, = European Economic Union, plus Norway, Iceland, plus for our purposes Switzerland
EMT	HCPC's Executive Management Team
EU	European Economic Union (formerly known as the "Common Market")
Europa Quality Print	Supplier of print and mailing services to HCPC
FReM	Financial Reporting Manual
FTP	Fitness to Practise
GP	Grandparenting
HSWPO	Health and Social Work Professions Order (2001)
HR	Human Resources
HW	Abbreviation for computer hardware
ISMS	I = Information Security Management System (ISMS) risk
Impact	The result of a particular event, threat or opportunity occuring. Scored between 1 least effect on HCPC and 5 maximum effect on HCPC.
ISO	International Standards Organisation (the global governing body for the Quality standards used by HCPC)
ISO 9001:2008	The ISO Quality Management Standard used by HCPC.
ISO 10002:2014	The ISO Complaints Management Standard used by HCPC.
ISO 27001:2013	The ISO Information Security Standard used by HCPC.
IT	Information Technology
Likelihood	Used to mean Probability of the event or issue occurring within the next 12 months
MIS	Management Information System
MOU	Memorandum of Understanding
NetRegulate	The bespoke computer application used to manage the application, registration and renewal processes, and publish the online register
OIC	Order in Council
OJEU	Official journal of the European Union
Onboarding	The process of bringing a new profession into statuatory regulation from HCPC's viewpoint
OPS	Operations
PSA	Formerly (CHRE), renamed Professional Standards Authority for Health and Social Care in the 2012 legislation.
PLG	Professional Liason Group
Probability	Likelihood, chance of occurring. Not the "mathematical" probability. Scored between 1 least likely and 5 most likely to occur within the next year.
Q	Q = Quality Management System (QMS) Risk
QMS	Quality Management System, used to record and publish HCPC's agreed management processes
Risk	Any uncertain event/s that could occur and have an impact on the achievement of objectives
Risk Owner	The person or entity that has been given the authority to manage a particular risk and is accountable for doing so.
Risk Score	Likelihood x Impact or Probability x Significance
SI	Statutory Instrument
Significance	Broadly similar to Impact
SSFS	Scheme Specific Funding Standard, a set of standards relating to pensions services
STD	Standards
SW	Abbreviation for computer software
VPN	Virtual Private Network, a method of securely accessing computer systems via the public internet

Information Security terms

ISO27001 term	Information Security area
ISO27001:2013 A5	Security Policy Management
ISO27001:2013 A6	Corporate Security Management
ISO27001:2013 A7	Personnel Security Management
ISO27001:2013 A8	Organizational Asset Management
ISO27001:2013 A9	Information Access Management
ISO27001:2013 A10	Cryptography Policy Management
ISO27001:2013 A11	Physical Security Management
ISO27001:2013 A12	Operational Security Management
ISO27001:2013 A13	Network Security Management
ISO27001:2013 A14	System Security Management
ISO27001:2013 A15	Supplier Relationship Management
ISO27001:2013 A16	Security Incident Mangement
ISO27001:2013 A17	Security Continuity Management
ISO27001:2013 A18	Security Compliance Management
C	Confidentiality
I	Integrity
A	Availability
x	Used in ISMS risks where not applied to C or I or A
TRT	Treat = Apply mitigations
TOL	Tolerate = Accept
TMT	Terminate = stop activity with risk
TSF	Transfer = move risk to other party
Systems Controls	Logical controls within systems
Operational Risk Management	Dept processes within BAU
Inter-dept quality assurance	Dept QA team activity where available (REG, FTP,
Near Miss Reporting	BPI investigation of reputational impact incidents

EDU)