Council, 7 December 2016

HCPC's Risk Appetite

Executive summary and recommendations

Introduction

The NAO recommends that organisations such as the HCPC define a risk appetite. An updated risk appetite statement and strategy were recently submitted to Audit Committee in September 2016. Audit Committee asked for risk appetite to be discussed at Council to validate our updated risk appetite.

Decision

The Council is asked to:-

- Discuss the level of HCPC's risk appetite in light of existing examples from the risk register and
- Agree HCPC's risk appetite, which is enclosed in the attached paper.

Background information [Sub-headings in Arial, 12 point, bold]

In the Audit Committee meeting on 6th September 2016, the Audit Committee received a paper on risk management strategy & risk appetite**.** The Committee noted that the HCPC's current risk appetite is low or risk averse. The Executive considers a low risk appetite is appropriate for HCPC's public protection remit for both operational and financial reasons. The Committee discussed the paper and agreed to postpone recommendation until it was considered by Council.

Resource implications

Annual departmental work plans.

Financial implications

Annual departmental work plans.

Appendices

i HCPC's risk appetite and risk management process
ii HCPC's risk matrix
iii HCPC's current risk register as an example

Date of paper

28th November 2016

Introduction

Risk appetite illustrates an organisations' willingness or lack of willingness to take greater risks for increased rewards with an acceptance that actions that may damage the organisation are more likely; alternately failure to take risks may cause stagnation. Selection of the appropriate risk appetite represents the correct balance, avoiding stagnation, but not unduly risking damage to the organisation.

The UK's lead on risk management, British Standards Institute (BSI), defines risk appetite as "Amount and type of risk that an organisation is prepared to seek, accept or tolerate". [BS31100]

The International Organization for Standardization (ISO) described risk appetite as "Amount and type of risk that an organisation is willing to pursue or retain". [ISO 31000 / Guide 73]

HCPC's current appetite for risk is low, or risk averse. The Executive believe the risk appetite is appropriate for a regulator. See Appendix i for the proposed risk appetite and risk management process.

Risk Register

The risk register is a list of all feasible, known risks associated with HCPC, and the mitigations to decrease the probability and consequences of those risks if and when they occur. Given our current low risk appetite, we aim to have mitigations in place to reduce the net likelihood and impact of each risk to a low level wherever possible.

One way of challenging HCPC's risk appetite is to question which risks might be removed, accepted without mitigation or mitigations might be changed; to be less risk averse and more accepting of a higher level of risk.

A copy of the current risk register is attached, for sample risks or mitigations to be considered in light of a potential lower risk aversion (more accepting of high risks).

Appendix i

HCPC's proposed risk appetite and risk management processes (Audit Committee, 6th September 2016)

1. A risk appetite is defined by the Council and will be reviewed if there is a significant change in our business. The current appetite is **low** or risk averse.

   Our objective is public protection, and we are a public body funded by registrants' fees. Operational failures could result in harm to the public, and financial failures could result in unexpected costs falling on registrants. Therefore a low risk appetite is appropriate for HCPC for both operational and financial reasons. For example, in operational choices where there is a trade off between quality and speed, we will tend to favour quality, or if there is a trade off between innovation and reliability, we will tend to favour reliability. In financial choices, we will tend to favour options that offer low returns but low volatility and limited downside over options that offer higher returns but with higher volatility and greater downside.

2. Risk management is broken down into operational areas, which in part map to departments or directorates at HCPC. For each operational area, we
   a. Identify all relevant risks
   b. Mitigate those risks to an appropriate, low level
   c. Invest mitigation resources in proportion to the level of risk

3. Risk owners at HCPC are Council, Chair of Council, Chief Executive & Registrar, members of EMT or Managers of departments.

4. Risks are assessed on an on going basis by risk owners.

5. Periodic planned review of risks, are input into the corporate risk register which is published to the Audit Committee and Council on a rolling 6 monthly basis. This is supported by a "Three lines of defence" Risk Assurance mapping model.

   i. Area A = Independent review / Assurance / Regulatory oversight
   ii. Area B = Functional oversight / Governance
   iii. Area C = Management Control & Reporting

   Further detail is indicated within the Risk Register where required.

6. Common agreed quantitative impact scales will be used consistently across the organisation.

7. Common, agreed quantitative likelihood scales are will be used consistently across the organisation.

8. Multiple mitigations are to be held for all risks where possible.

9. Realised risks are subsequently assessed against the appropriate risk register entry to assess the effectiveness of the Risk Management process.

10. Historic realisation of risks, may be used to inform the forward looking risk register where appropriate.

11. A core document, the “Risk Register” holds all the key information required to manage the organisational risks at any one time.

12. The Risk Register will be used by the internal audit function to suggest areas of interest for audit.

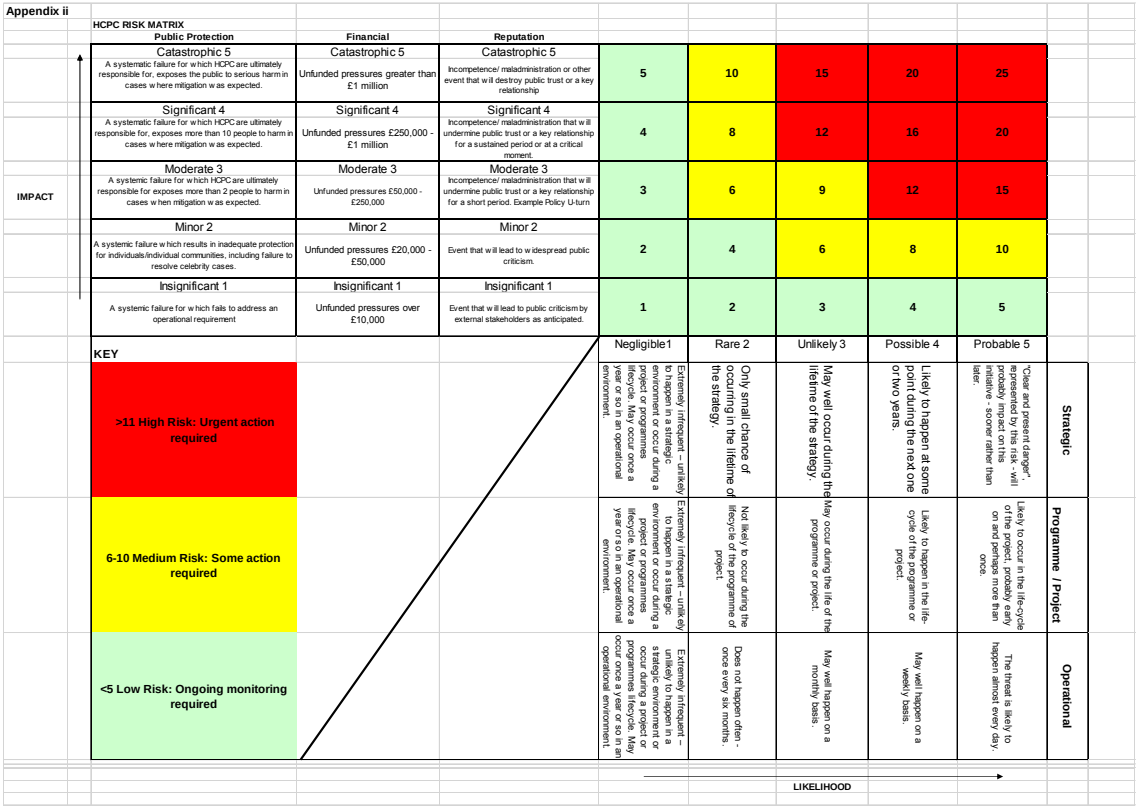
13. Major projects have their own risk registers managed by the Project management team, but risk assessed by the Project Board

14. Very high profile project risks may be managed by the Business Process Improvement function at the request of the Chief Executive & Registrar. These risk registers may be confidential to the Audit Committee or Council

15. Internal Audit contractors will be appointed for no more than four years.

16. Internal Audit contractors will not also be appointed as External Auditors.

Appendix ii



Appendix ii

HCPC RISK MATRIX

IMPACT	Public Protection	Financial	Reputation						
	Catastrophic 5 A systematic failure for which HCPC are ultimately responsible for, exposes the public to serious harm in cases where mitigation was expected.	Catastrophic 5 Unfunded pressures greater than £1 million	Catastrophic 5 Incompetence/ maladministration or other event that will destroy public trust or a key relationship	5	10	15	20	25	
	Significant 4 A systematic failure for which HCPC are ultimately responsible for, exposes more than 10 people to harm in cases where mitigation was expected.	Significant 4 Unfunded pressures £250,000 - £1 million	Significant 4 Incompetence/ maladministration that will undermine public trust or a key relationship for a sustained period or at a critical moment.	4	8	12	16	20	
	Moderate 3 A systemic failure for which HCPC are ultimately responsible for exposes more than 2 people to harm in cases when mitigation was expected.	Moderate 3 Unfunded pressures £50,000 - £250,000	Moderate 3 Incompetence/ maladministration that will undermine public trust or a key relationship for a short period. Example Policy U-turn	3	6	9	12	15	
	Minor 2 A systemic failure which results in inadequate protection for individuals/individual communities, including failure to resolve celebrity cases.	Minor 2 Unfunded pressures £20,000 - £50,000	Minor 2 Event that will lead to widespread public criticism.	2	4	6	8	10	
	Insignificant 1 A systemic failure for which fails to address an operational requirement	Insignificant 1 Unfunded pressures over £10,000	Insignificant 1 Event that will lead to public criticism by external stakeholders as anticipated.	1	2	3	4	5	
				Negligible1	Rare 2	Unlikely 3	Possible 4	Probable 5	

KEY

>11 High Risk: Urgent action required	Extremely infrequent – unlikely to happen in a strategic environment or occur during a programmes lifecycle. May occur once a year or so in an operational environment.	Only small chance of occurring in the lifetime of the strategy.	May well occur during the lifetime of the strategy.	Likely to happen at some point during the next one or two years.	"Clear and present danger", represented by this risk - will probably impact on this initiative - sooner rather than later.	**Strategic**
6-10 Medium Risk: Some action required	Extremely infrequent – unlikely to happen in a strategic environment or occur during a programmes lifecycle. May occur once a year or so in an operational environment.	Not likely to occur during the lifecycle of the programme of project.	May occur during the life of the programme or project.	Likely to happen in the life-cycle of the programme or project.	Likely to occur in the life-cycle of the project, probably early on and perhaps more than once.	**Programme / Project**
<5 Low Risk: Ongoing monitoring required	Extremely infrequent – unlikely to happen in a strategic environment or occur during a programmes lifecycle. May occur once a year or so in an operational environment.	Does not happen often - once every six months.	May well happen on a monthly basis.	May well happen on a weekly basis.	The threat is likely to happen almost every day.	**Operational**

LIKELIHOOD

Risk Register & Risk Treatment Plan

Marc Seale, Chief Executive & Registrar
Report to Audit Committee, (Sept 2016)

hcpc health & care professions council

July 2016 Risk Assessment

THE HEALTH AND CARE PROFESSIONS COUNCIL

"Top 10" Risks (High & Medium after mitigation)

Historic Risk Scores

	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Mitigation I	Mitigation II	Mitigation III	CURRENT RISK SCORE	Feb-16	Sep-15	Feb-15	Sep-14	Feb-14	Sep-13	Feb-13				
2.7	Interruption to electricity supply (pre-mit 16) ISMS RISK	Office Services Mgr	Relocate to other buildings on site	If site wide longer than 24 hours invoke DR Plan	-	**High**	**High**	**High**	**High**	**High**	**High**	**High**	**High**				
1.8	Transfer of SW (England) from HCPC to New Reg	Chief Executive	Major Project Risk Register	Managed timetable	Project Plan experience	**Medium**											
13.3	Tribunal exceptional costs (pre-mit 25)	FTP Director	Quality of operational processes	Accurate and realistic forecasting	Quality of legal advice	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**				
17.9	Loss of ISO27001 :2013 certification (pre-mit 20)	Hd of Business Process Improv & Asset Owners	Culture, follow procedures, report errors, training and awareness as required	Standard Operating Procedures and prevention of overwriting systems	Extend ISO systems as required	**Medium**	**Medium**										
2.11	Basement flooding (pre-mit 16)	Office Services Mgr	Flood barrier protection to prevent ingress	Periodic descaling of drainage	Investigate benefits of Non Return valves in drain gratings.	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**				
13.4	Rapid increase in number of allegations and resultant legal costs (pre-mit 16)	FTP Director	Accurate and realistic budgeting	Resource planning	-	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**					
1.5	Loss of reputation (pre-mit 15)	Chief Executive & Chair	Quality of governance procedures	Quality of operational procedures	Dynamism and quality of Comms strategy	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**				
12.1	Judicial review of HCPC's implimentation of HSWPO including Rules, Standards & Guidance (pre-mit 15)	Chief Executive	Consultation. Stds determined by PLG's. Agreement by Council.	Appropriate legal advice sought	-	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**				
15.28	PSA fee increases substantially, placing significant financial pressure on HCPC (pre-mit 12)	Finance Director	Consider increase in fees	Legislative and operational adjustments	-	**Medium**	**Medium**										
7.6	Loss or significant change to funding, commissioning and placement opportunities for approved programmes	Director of Education	Operational processes (approval, monitoring and complaints about an approved programme)	Partnerships with Visitors and professional groups.	Regular training of employees and visitors	**Medium**											

Risks listed in order of CURRENT RISK SCORE, then PRE_MITIGATION SCORE

Changes since the previous iteration of HCPC's Risk Register

Category	Ref#	Description	Nature of change in this version
Strategic	1.4	Update Mitigation I	Add word effective
	1.4	Update Mitigation II	Add phrase "at all levels of the organisation"
	1.6	Update Mitigation II	Add "and Council"
	1.7	Update Mitigation I	Add "Council members and partners"
	1.7	Update Mitigation II	Add "Council members and partners"
Operations	2.11	Update Mitigations II & III	Add Descaling and Non return valves option
	2.x	Change Facilities Manager to Office Services Manager	Update job title throughout
Corporate Governance	4.1	Update Mitigation III	Change to "Robust & effective recruitement process"
	4.4	Update Mitigation III	Add "Robust discussion at annual appraisal"
	4.6	Update Mitigation III	Add "External appraisal and effective feedback from fellow Council members"
	4.9 & 4.11	Update Mitigation II	Change Extranet to iPad
	4.16	Update Mitigation III	Change to Effective engagement with PSA throughout process
Policy & Standards	14.2	Add Commisioned research to 14.2	Add Commisioned research to mitigation I of 14.2
		Information Security Management System risks	ISMS Controls indicated for information security ricks
App ii Risk Matrix defns		Historic financial impact levels removed from Risk Matrix defns	Remove greyed out values
App iii Strat Obj		Strategic Objectives mapped to indivudual risks	Add risk per Strategic Objective where specified

Overview of Risk Management and Risk Treatment process

Throughout the year exisiting risks are continually monitored and assessed by Risk Owners against Likelihood, and Impact on HCPC, the effectiveness of mitigations and the levels of residual risk.

Future risks are also documented, evaluated and monitored against the same criteria.

Every six months these changes and additions to risks are updated in the risk register and formally documented by the Director of Operations or Head of Business Process Improvement, and the Top Ten Risks (High & Medium only after mitigation) are recorded.

Individual risks are linked to the current Statement of Applicability by the ISO27001 Clauses noted in the ISMS Risks column on each page.
Strategic Objectives are linked to individual risks where applicable.

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Strategic

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
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									
	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,									
	Strategic	**I A5, 18**	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
	Strategic		1.4	Failure to maintain a relationship with PSA	Chief Executive & Chair	5	1	5	HCPC Chair and Chief Executive **effective** relationship with PSA	Communications **at all levels of the organisation**	-	Low	Low
	Strategic	**I A5,**	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
	Strategic		1.6	Failure to abide by current Equality & Diversity legislation	Chief Executive	4	2	8	Equality & Diversity scheme	Implementation of scheme for employees, Implementation of scheme for **Council members and** partners	Equality & Diversity working group	Low	Low
	Strategic		1.7	Failure to maintain HCPC culture	Chief Executive	5	2	10	Behaviour of all employees, **Council members and partners**	Induction of new employees, **Council members and partners**	Internal communication	Low	Low
	Strategic		1.8	Transfer of SW (England) from HCPC to New Reg	Chief Executive	5	3	15	Major ProjectRisk Register	Managed timetable	Project Plan experience	Medium	Medium

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2016

Operations

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
2	**Operations**	**I A11, 17.2.1**	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
	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									
	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									
	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
	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
	Operations	**I A11**	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									
	Operations	**I A11.2.2**	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
	Operations		2.8	Interruption to gas supply	Office Services Mgr	1	2	2	Temporary heaters to impacted areas	-	-	Low	Low
	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
	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 telephone lines from the two exchanges with different media types	Low	Low
	Operations	**I A11, 17**	2.11	Basement flooding	Office Services Mgr	4	4	16	Flood barrier protection to prevent ingress	Periodic descaling of drainage	Investigate benefits of Non Return valves in drain gratings.	Medium	Medium
	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
	Operations		2.14 (formerl y11.5)	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									
	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

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Communications

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
3	**Communications**		3.1	Failure to inform public Article 3 (13)	Director of Comms	5	1	5	Delivery of communications strategy.	Delivery of aspects of communications workplan, specifically public information campaigns, multi media advetising, distribution of public information materials, and web.	-	Low	Low
	Communications		3.2	Loss of support from Key Stake holders including professional bodies, employers or government	Director of Comms	5	3	**15**	Delivery of communications strategy, supporting the HCPC strategy	Delivery of aspects of communications work plan, specifically stakeholder activities	Quality of Operational procedures	Low	Low
				Links to 1.5									
	Communications		3.3	Inability to inform stakeholders following crisis	Director of Comms	4	1	4	Invoke Business Continuity Plan (BCP)	Up to date Comms BCP available	-	Low	Low
	Communications		3.4	Failure to inform Registrants Article 3 (13)	Director of Comms	5	1	5	Delivery of communications strategy	Delivery of aspects of communications workplan, specifically, Meet the HCPC events, campaigns, Registrant Newsletter, Profesional media and conference attendance . Publications and web.	Quality of Operational procedures	Low	Low
	Communications		3.5	Publication of material not approved for release	Director of Comms	4	2	8	Delivery of communications plan	Adherence to ISO9001 processes	Adherence to operational plans, eg forward planner	Low	Low
	Communications		3.6	Failure to achieve engagement in the four home countries	Director of Comms	?	?		Delivery of communications plan	Networking with Home Country Departments of Health		Low	New

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Corporate Governance

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
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 recruitement process**	Low	Low
				Links to 4.4									
	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
	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
	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									
	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
	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 feedbak from fellow Council members**	Low	Low
	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
	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
	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									
	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									
	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
	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
	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	Department training	Low	Low
	Corporate Governance	**I A18.1.1**	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
	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
	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

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Information Technology

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
5	**IT**	**I A12,13,14, 9**	5.1	Software Virus damage	Director of IT	4	5	20	Anti-virus software deployed at several key points.Application of security patches in a timely manner	Adherence to IT policy, procedures and training	Regular externally run security penetration tests.	Low	Low
				Links to 2.3, 10.2									
	IT	**I A12,14, 17.1, 14**	5.2	Technology obsolescence, (Hard/SoftWare)	Director of IT	2	2	4	Delivery of the IT strategy including the refresh of technology.	Employ small core of mainstream technology with recognised support and maintenance agreements	Accurately record technology assets.	Low	Low
				Links to 2.6, 10.2									
	IT	**I A9,8,13**	5.3	Fraud committed through IT services	Director of IT	3	3	9	Appropriate and proportionate access restrictions to business data. System audit trails.	Regular, enforced strong password changes.	Regular externally run security tests.	Low	Low
				Links to 10.2 and 17.1									
	IT	**I A17, 14,12**	5.4	Failure of IT Continuity Provision	Director of IT	4	3	12	Annual IT continuity tests	IT continuity plan is reviewed when a service changes or a new service is added	Appropriate and proportionate technical solutions are employed. IT technical staff appropriately trained.	Low	Low
	IT	**I A9.4, 9.2, 7**	5.5	Malicious damage from unauthorised access	Director of IT	4	5	20	Security is designed into the IT architecture, using external expert consultancy where necessary	Regular externally run security penetration tests.	Periodic and systematic proactive security reviews of the infrastructure. Application of security patches in a timely manner. Physical access to the IT infrastructure restricted and controlled.	Low	Low
	IT	**I A11.2.2 A17.1.2**	5.6	Data service disruption (via utility action)	Director of IT	5	1	5	Redundant services	Diverse routing of services where possible	Appropriate service levels with utility providers and IT continuity plan	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2016

Partners

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
6	**Partners**		6.1	Inability to recruit and retain suitable Partners	Partner Manager	3	3	9	Targetted recruitment strategy.	Appropriate fees for partner services and reimbursement of expenses.	Efficient and effective support and communication from the Partner team.	Low	Low
				Links to 4.10, 11.3, 7.3,									
	Partners		6.2	Incorrect interpretation of law by Partners resulting in PSA review	Director of FTP, Director of Education, Head of Registration, Partner Manager	2	4	8	Partner training and newsletters	Legal Advice	Regular appraisal system	Low	Low
	Partners		6.3	Health & Safety of Partners	Partner Manager	3	2	6	H&S briefing at start of any HCPC sponsored event.	Liability Insurance	-	Low	Low
				Links to 4.9									
	Partners		6.4	Partners poor performance and / or conduct	Director of FTP, Director of Education, Head of Registration, Partner Manager	4	3	12	Regular training	Regular appraisal system	Partner Complaints Process & Partner Code of Conduct	Low	Low
	Partners		6.5	Incorrect interpretation of HSWPO by HCPC in use of Partners	Director of FTP, Director of Education, Head of Registration, Partner Manager	3	2	6	Legal Advice	Clearly defined Quality Management processes and policies	Correct selection process and use of qualified partners	Low	Low
	Partners		6.6	Adequate number and type of partner roles	Partner Manager, Director of FTP, Director of Education, Head of Registration	3	2	6	Regular review of availability of existing pool of partners to ensure requirements are met.	Annual forecasting of future partner requirements to ensure that they are budgetted for.	Rolling partner agreements across professions for Panel Member and Panel Chair to ensure adequate supply in line with the eight year rule.	Low	Low
	Partners		6.7	User departments using non-active partners	Partner Manager, Director of FTP, Director of Education, Head of Registration	3	3	9	Notification of partner resignations to user departments.	Current partner lists available to user departments on shared drive.	Daily Email notificaton of partner registrant lapse	Low	Low
	Partners		6.8	Expense claim abuse by Partners	Partner Manager, Director of FTP, Director of Education, Head of Registration	2	2	4	Budget holder review and authorisation process	Comprehensive Partner agreement	Challenge of non standard items by, Finance department and Partner Department	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Education

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jul 2015
7	**Education**		7.1	Failure to detect low education providers standards	Director of Education	4	2	8	Operational processes (approval, monitoring and complaints about an approved programme)	Regular training of employees and visitors	Memorandums of understandings with other regulators (e.g. CQC and Care Councils)	Low	Low
				Links to 1.1 , 4.3, 6.4									
	Education		7.2	**Education providers disengaging with process**	Director of Education	3	3	9	Legal powers (HSWPO 2001)	Delivery of Education Dpt supporting activities as documented in regular work plan	Stakeholder monitoring	Low	Low
				Links to 1.1									
	Education		7.3	Inability to conduct visits and monitoring tasks	Director of Education	4	2	8	Adequate resourcing, training and visit scheduling	Approvals & monitoring processes	Temporary staff hire to backfill or clear work backlogs	Low	Low
				Links to 1.1, 6.1, 11.2 & 11.3									
	Education		7.4	Loss of support from Education Providers	Chief Executive or Director of Education	5	2	10	Delivery of Education strategy as documented in regular work plan	Partnerships with Visitors and professional groups.	Publications, Newsletters, website content, inclusion in consultations and relevant PLGs, consultations with education providers	Low	Low
				Links to 1.1, 14.2									
	Education	**I A12,13,14 15**	7.5	**Protracted service outage following Education system failure**	Director of IT	4	2	8	Effective backup and recovery processes	In house and third party skills to support system	Included in future DR/BC tests	Low	Low
	Education		7.6	Loss or significant change to funding, commissioning and placement opportunities for approved programmes	Director of Education	3	4	12	Operational processes (approval, monitoring and complaints about an approved programme)	Partnerships with Visitors and professional groups.	Regular training of employees and visitors	Med	Low
	Education		7.7	Monitoring processes not effective	Director of Education	3	2	6	Well documented processes	Trained executive & visitors	Communication with education providers	Low	NEW

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Project Management

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the on-going risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
8	**Project Management**		8.1	Fee change processes not operational by required date	Director of Finance Project Portfolio Manager	3	3	9	Project is managed as part of major projects portfolio & managed in accordance with HCPC Project Management process	Project progress monitored by EMT & stakeholders	-	Low	Low
				Links to 1.1, 15.3									
	Project Management		8.2	Failure to regulate a new profession or a post-registration qualification as stipulated by legislation	Project Lead Project Portfolio Manager	5	2	10	Project is managed as part of major projects portfolio & managed in accordance with HCPC Project Management process	Project progress monitored by EMT & stakeholders	Assess lessons to be learned from previous projects	Low	Low
				Links to 1.1, 15.3									
	Project Management	**I A14, 15**	8.13	Failure to build a system to the the Education departments requirements	Director of Education Project Portfolio Manager	3	4	12	Project is managed as part of major projects portfolio & managed in accordance with HCPC Project Management process	Project progress monitored by EMT & stakeholders	Ensure robust testing including load	Low	Low
	Project Management	**I A14, 15**	8.14	Failure to deliver a system to the HR & Partners departments requirements	Director of HR Project Portfolio Manager	3	4	12	Project is managed as part of major projects portfolio & managed in accordance with HCPC Project Management process	Project progress monitored by EMT & stakeholders	Project Initiation stage to pay particular attention to project scope and breadth/reach of project	Low	Low
	Project Management	**I A7.2.1**	8.17	Organisation wide resourcing may impact project delivery	EMT & Project Portfolio Manager	3	4	12	Manage resources accordingly	Accept changes to planned delivery		Med	Med
	Project Management	**I A14, 15**	8.19	Failure to build a system to the Registrations department's requirements	Director of Operations & Project Portfolio Manager	5	4	20	Project is managed as part of major projects portfolio & managed in accordance with HCPC Project Management process	Project progress monitored by EMT & stakeholders	Ensure robust testing including load	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Quality Management

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
9	**Quality Management.**		9.1	Loss of ISO 9001:2008 Certification	Director of Operations, Head of Business Improvement	4	3	**12**	Regular & internal audits	QMS standards applied across HCPC	Management buy - in	Low	Low
				Links to 2.3, 10.3									
	Quality Management.	**I A7.1.2**	9.2	Employees non-compliance with established Standard Operating Proceedures	EMT	5	2	**10**	Culture, follow procedures and report errors	Standard Operating Procedures and prevention of overwriting systems	Extend ISO systems as required	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2016

Registrations

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
10	**Registration**		10.1	Customer service failures	Director of Operations, Head of Registration	5	4	**20**	Accurate staffing level forecasts	Adequate staff resourcing & training	Supporting automation infrastructure eg call centre systems, NetRegulate system enhancements, registration re-structure; **externally sourced registrant surveys**	Low	Low
				Links to 11.1, 11.2									
	Registration		10.2	Protracted service outage following a NetRegulate Registration 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
				Links to 5.1-5.3 and 17.1									
	Registration		10.3	Inability to detect fraudulent applications	Director of Operations, Head of Registration	5	2	10	Financial audits, system audit trails	Policy and procedures supported by internal quality audits	Validation of submitted information, Education & ID checks. **NHS Protect fraud measurement exercises ongoing**	Low	Low
				Links to 9.1, 17.1 and 17.2									
	Registration		10.4	Backlogs of registration and applications	Director of Operations, Head of Registration	4	3	**12**	Continually refine model of accurate demand-forecasting, to predict employees required to prevent backlogs, and service failures	Process streamlining	Match resource levels to meet demand & delivery published Service Standards	Low	Low
				Links to 1.1									
	Registration		10.5	Mistake in the Registration process leading to liability for compensation to Registrant or Applicant	Director of Operations, Head of Registration	5	2	10	Audits by Registration Management, system audit trails, external auditors	Professional indemnity insurance. Excess £2.5K. Limit £1M. (Doesn't cover misappropriation of funds)	Policy and procedures supported by ISO quality audits and process controls/checks	Low	Low
18	**Registration**		10.6 (18.1-7.5)	CPD processes not effective	Director of Operations, Head of Registration	4	2	8	Well documented processes	Appropriately trained members of the registrations team	Monitor and regular feedback to the Education & Training Committee	Low	Low
				Links to 1.1									
	Registration		10.7 (13.7)	Failure to manage Registration Appeals effectively and efficiently	Director of Operations, Head of Registration	4	2	8	Well documented processes	Appropriately trained members of the registrations team	Monitor and regular feedback from the Reg Appeals panel	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

HR

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
11	**HR**		11.1	Loss of key HCPC employees, excluding Chief Exec	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
	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									
	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									
	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									
	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
	HR		11.7	Employee and ex-employee litigation	HR Director	4	3	**12**	Line manager training	Keeping HR policies and processes in line with employment legislation	Employee surveys, Exit Interviews, Employee Assistance Programme, Management Development Programme.	Low	Low
	HR	**I A7, 8**	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									
	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
	HR		11.10	Loss of Chief Executive & Registrar	Chair	5	2	**10**	Succession Plan	Development of internal Executive team	Good communication with Chair	Low	Low
				Includes Auto enrolment pensions									

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Legal

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
12	**Legal**		12.1	Judicial review of HCPC's implimentation of HSWPO including Rules, Standards & Guidance	Chief Executive	5	3	**15**	Consultation. Stds determined by PLG's. Agreement by Council.	Appropriate legal advice sought	-	Medium	Medium
				Links to 1.2, 14.1, 14.2									
	Legal	**I A18**	12.2	Legal challenge to HCPC operations	Chief Executive	4	4	**16**	Legal advice and ISO	**Pre-emptive and on-going communications concerning legal basis and implimentation of the HSWPO**	-	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Fitness to Practise

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
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									
	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
	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									
	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
	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
				13.7 moved to 10.7									
	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
	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									
	Fitness to Practise	**I A12,13, 14, 16, 17**	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

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2016

Policy & Standards

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
14	**Policy & Standards**		14.1	Incorrect process followed to establish stds/guidance/policy eg no relevant Council decision	Policy & Stds Director	4	2	8	Legal advice and sign off sought on processes	Appropriately experienced and trained members of Policy team.	Quality mgt system & processes	Low	Low
				Links to 12.1									
	Policy & Standards		14.2	Inappropriate stds/guidance published eg stds are set at inappropriate level, are too confusing or are conflicting	Council/committees	4	1	4	Use of commissioned research, professional liaison groups, and Council and committees including members with appropriate expertise	Appropriately experienced and trained members of Policy team.	Consultation with stakeholders & legal advice sought	Low	Low
	Policy & Standards		14.3	Changing/evolving legal advice rendering previous work inappropriate	Policy & Stds Director	4	2	8	Use of well-qualified legal professionals. Regular reviews.	Legal advice obtained in writing.	Appropriately experienced and trained members of Policy team and others eg HR.	Low	Low
	Policy & Standards		14.4	Inadequate preparation for a change in legislation (Health Professions Order, or other legislation affecting HCPC)	EMT	3	1	3	EMT responsible for remaining up to date relationships with governemnt depts and agencies.	HCPC's 5 year planning process	Legal advice sought	Low	Low
	Policy & Standards		14.5	PLG member recruitment without requisite skills and knowledge	Policy & Stds Director HCPC Chair, Director of Council & Committee Services(?)	4	1	4	Skills and knowledge identified in work plan	Recruitment policy	Council Scrutiny of PLG result	Low	Low
				Lnks to 4.10									
	Policy & Standards		14.6	Loss of Corporate Memory	Policy & Stds Director	3	3	9	Maintain appropriate records of project decisions	Appropriate hand over and succession planning	Department training	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Finance

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
15	**Finance**		15.1	Insufficient cash to meet commitments	Finance Director	5	1	5	Reserves policy specifies minimum cash level to be maintained throughout the year. Cash flow forecast prepared as part of annual budget and 5 year plan assesses whether policy minimum level will be met.	Regular cash forecasts and reviews during the year	Fee rises and DoH grant applications as required.	Low	Low
	Finance		15.2	Unexpected rise in operating expenses	EMT	4	1	4	Budget holder accountability for setting budgets and managing them. Timely monthly reporting and regular budget holder reviews held. EMT review of the monthly variances year to date.	Six and nine month reforecasts with spending plan revisions as feasible and appropriate. FTP costs mainly incurred towards the end of the lifecycle of a case, so increase in case pipeline would give early warning of rise in FTP costs.	Capped FTP legal case costs.	Low	Low
				Link to 13.1									
	Finance		15.3	Major Project Cost Over-runs	Project Lead / EMT	4	2	8	Effective project specification including creating decision points. Effective project management and timely project progress reporting (financial and non financial).	Project budgets have 15% contingency. Project exception reports including revised funding proposal is presented to EMT for approval.	EMT review of the project spending variances to date	Low	Low
	Finance	**I A7, 8, 9**	15.7	Registrant Credit Card record fraud/theft	Finance Director	2	2	4	Compliance with PCI standards.	Limited access to card information	Professional Indemnity & fidelity (fraud) insurance for first £250k of loss	Low	Low
				Links to 5.3									
	Finance		15.9	Mismatch between Council goals & approved financial budgets	Chief Executive	4	2	8	Close and regular communication between the Executive, Council and its Committees.	Adequate quantification of the budgetary implications of proposed new initiatives	Use of spending prioritisation criteria during the budget process	Low	Low
				Links to 1.1									
	Finance	**I A8, 11,**	15.12	Unauthorised removal of assets (custody issue)	Office Services Mgr & IT Director	2	2	4	Building security including electronic access control and recording and CCTV. IT asset labeling & asset logging (issuance to employees)	Fixed Asset register itemising assets. Job exit procedures (to recover HCPC laptops, blackberries, mobile phones etc). Regular audits. Whistleblowing policy.	Computer asset insurance.	Low	Low
	Finance	**I A8, 11,**	15.13a	Theft or fraud	Finance Director	3	2	6	Well established effective processes, incl segregation of duties and review of actual costs vs budgets.	Regular audits; whistleblowing policy	Professional Indemnity & fidelity (fraud) insurance for first £250k of loss	Low	Low
				Incorporates aspects of previous risks 15.10 and 15.11									
	Finance		15.18	PAYE/NI/corporation tax compliance	Finance Director	2	3	6	Effective payroll process management at 3rd party. Finance staff attend payroll & tax updates	Professional tax advice sought where necessary, including status of CCMs and partners	PAYE Settlement Agreement in place with HMRC relating to Category One Council and Committee members.	Low	Low
	Finance		15.20	Bank insolvency: permanent loss of deposits or temporary inability to access deposits	Finance Director	5	1	5	Investment policy sets "investment grade" minimum credit rating for HCPC's banks and requires diversification - cash spread across at least two banking licences			Low	Low
	Finance		15.21	Financial distress of key trade suppliers causes loss of business critical service	Finance Director	4	2	8	Financial health of new suppliers above OJEU threshold considered as part of OJEU PQQ process. Ongoing financial monitoring of key suppliers	Escrow agreements	Alternative suppliers where possible, eg transcription services framework	Medium	Medium
	Finance		15.22	Payroll process delay or failure	Finance Director	2	2	4	Outsourced to third party. Agreed monthly payroll process timetable (with slack built in). If process delayed, payment may be made by CHAPS (same day payment) or cheque.	Hard copy records held securely. Restricted system access.		Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Finance

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
	Finance		15.24	Failure to apply good procurement practice (contracts below OJEU threshold) leads to poor value for money and/or criticism	Finance Director & Procurement Mgr	2	2	4	Approved procurement policy. Legal advice on ISO9001 compliant process design.	Internal monitoring of Tendering and contract process use.	New suppliers process as "backstop" to failure.	Low	Low
	Finance		15.25	Failure to adhere to OJEU Procurement and Tendering requirements leads to legal challenge and costs	Finance Director & Procurement Mgr	4	2	8	Use Framework Agreements as standard practise at HCPC	Robust OJEU specific processes agreed by legal advisors. Legal oversight of OJEU related material created by HCPC	Legal oversight of OJEU scoring and supplier communication	Low	Low
	Finance		15.26	Budgeting error leads to overcommitment of funds	Finance Director	4	2	8	Income and FTP costs are budgeted for on FAST standard models. Payroll costs are budgeted for post by post. Cautious assumptions used in relation to income and payroll.	Budgets are prepared by departments and then reviewed by Finance. Budgets for coming year baselined vs current year budget and forecast	Budgets are discussed/challenged by EMT at annual pre-budget setting review	Low	Low
	Finance		15.27	Payment error leads to irrecoverable funds	Finance Director	3	2	6	Extensive use of preferred suppliers with bank account details loaded into Sage.	System controls over changing payee bank details	Payment signatory reviews of payment runs	Low	Low
	Finance		15.28	PSA fee increases substantially, placing significant financial pressure on HCPC	Finance Director	4	3	12	Consider increase in fees	Legislative and operational adjustments		Medium	Medium

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Pensions

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
16	**Pensions**		16.2	Non compliance with pensions legislation	Finance Director and HR Director	3	2	6	HCPC pension scheme reviewed for compliance with pensions legislation including auto enrolment	HR and Finance staff briefed on regulations	Advice from payroll provider. Seek specialist pensions legal advice as required.	Low	Low
	Pensions		16.3	Increase in the Capita Flexiplan funding liability resulting from scheme valuation deficiency	Finance Director	3	2	6	Plan is closed to new members so there is only a limited set of circumstances that could give rise to an increase in the liability	Initial employer contributions to the Plan deficit were set on prudent basis	Monitor the performance of the Plan through periodic employers' meetings	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL

RISK ASSESSMENT & RISK TREATMENT PLAN July 2016

Information Security

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2016	Likelihood before mitigations Jul 2016	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2016	RISK score after Mitigation Jan 2016
17	**Information Security**	**I A6,8,9 12,14**	17.1	Loss of information from HCPC's electronic databases due to inappropriate removal by an employee	EMT, Director of IT and Director of Operations	5	3	**15**	Access is restricted to only the data that is necessary for the performance of the services. Employment contract includes Data Protection and Confidentiality Agreement	Adequate access control procedures maintained. System audit trails. Training where appropriate.	Laptop encryption. Remote access to our infrastructure using a VPN . Documented file encryption procedure . Maintain ISO27001	Low	Low
				Links to 5.3. Incl old 17.6									
	Information Security	**I A11,8, 7,15,16, 17**	17.2	HCPC Document & Paper record Data Security	EMT; Head of Business Improvement	5	3	**15**	Use of locked document destruction bins in each dept. Use of shredder machines for confidential record destruction in some depts e.g. Finance.	Data Protection agreements signed by the relevant suppliers. Dept files stored onsite in locked cabinets. Training where appropriate (Employees & Partners)	Regarding Reg Appln forms processing, employment contract includes Data Protection Agreement	Low	Low
				Links to 15.7									
	Information Security	**I A15, 8, 13**	17.3	Unintended release of electronic or paper based information by external service providers.	EMT, Director of IT and Director of Operations	5	3	**15**	Access is restricted to only the data that is necessary for the performance of the services.	Effective system processes including secure data transfer and remote access granted only on application and through secure methods.	Data Processor agreements signed by the relevant suppliers. Maintain ISO27001	Low	Low
	Information Security	**I A18, 15, 13**	17.4	Inappropriate data received by HCPC from third parties	Director of Ops, and Director of FTP	5	2	10	Read only, password protected access by a restricted no of FTP employees to electronic KN data.	Registrant payments taken in compliance with Payment Card Industry (PCI) Security standards ie with quarterly PCI testing.	Ensure third party data providers e.g. professional bodies provide the data password protected/encrypted/door to door courier/registered mail/sign in sign out as appropriate.	Low	Low
	Information Security	**I A15, 8**	17.5	Loss of physical data dispatched to and held by third parties for the delivery of their services	Director of Ops and Hd of Business Process Improv	5	3	**15**	Data Protection/Controller agreements signed by the relevant suppliers. Use of electronic firewalls by suppliers.	Use of transit cases for archive boxes sent for scanning or copying and sign out procedures.	-	Low	Low
	Information Security	**I A9, 12, 13, 15**	17.6	Loss of Registrant personal data by the registration system (NetRegulate) application support provider in the performance of their support services (specific risk).	Director of IT and Director of Operations,	5	3	**15**	Access to and export of personal data is restricted to only that which is necessary for the performance of the services.	Effective system processes including secure data transfer and remote access granted only on application and through secure methods.	Data processor side letter specifying obligations and granting a limited indemnity.	Low	Low
	Information Security	**I A8**	17.7	Incorrect risk assessment of Information Assets	Hd of Business Process Improv & Asset Owners	4	2	**8**	Identification and collection of information risk assets	Regular audit and review of information risk assets by Hd of BPI	Regular identification and review of information risk assets by Hd of BPI	Low	Low
	Information Security	**I A6, 7, 8, 9**	17.8	Loss of personal data by an HCPC Contractor, Partner, Council or Committee member.	EMT	5	3	**15**	Access to and export of personal data is restricted to only that which is necessary for the performance of the services.	Effective system processes including secure data transfer and remote access granted only on application and through secure methods. Training where appropriate.	Maintain ISO27001	Low	Low
	Information Security	**I A5**	17.9	Loss of ISO 27001:2013 Certification	Hd of Business Process Improv & Asset Owners	5	4	**20**	Culture, follow procedures, report errors, training and awareness as required	Standard Operating Procedures and prevention of overwriting systems	Extend ISO systems as required	Med	Med

Appendix i

Glossary & Abbreviations

Term	Meaning
AGM	Annual General Meeting
BCP / BCM	Business Continuity Plan / Business Continuity Management (Disaster Recovery and associated processes)
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 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	An 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
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

Appendix ii

HCPC RISK MATRIX

IMPACT	Public Protection	Financial	Reputation					
	Catastrophic 5 A systematic failure for which HCPC are ultimately responsible for, exposes the public to serious harm in cases where mitigation was expected.	Catastrophic 5 Unfunded pressures greater than £1 million	Catastrophic 5 Incompetence/ maladministration or other event that will destroy public trust or a key relationship	**5**	**10**	**15**	**20**	**25**
	Significant 4 A systematic failure for which HCPC are ultimately responsible for, exposes more than 10 people to harm in cases where mitigation was expected.	Significant 4 Unfunded pressures £250,000 - £1 million	Significant 4 Incompetence/ maladministration that will undermine public trust or a key relationship for a sustained period or at a critical moment.	**4**	**8**	**12**	**16**	**20**
	Moderate 3 A systemic failure for which HCPC are ultimately responsible for exposes more than 2 people to harm in cases when mitigation was expected.	Moderate 3 Unfunded pressures £50,000 - £250,000	Moderate 3 Incompetence/ maladministration that will undermine public trust or a key relationship for a short period. Example Policy U-turn	**3**	**6**	**9**	**12**	**15**
	Minor 2 A systemic failure which results in inadequate protection for individuals/individual communities, including failure to resolve celebrity cases.	Minor 2 Unfunded pressures £20,000 - £50,000	Minor 2 Event that will lead to widespread public criticism.	**2**	**4**	**6**	**8**	**10**
	Insignificant 1 A systemic failure for which fails to address an operational requirement	Insignificant 1 Unfunded pressures over £10,000	Insignificant 1 Event that will lead to public criticism by external stakeholders as anticipated.	**1**	**2**	**3**	**4**	**5**

KEY

>11 High Risk: Urgent action required

6-10 Medium Risk: Some action required

<5 Low Risk: Ongoing monitoring required

LIKELIHOOD	Negligible1	Rare 2	Unlikely 3	Possible 4	Probable 5
Strategic	Extremely infrequent – unlikely to happen in a strategic environment or occur during a project or programmes lifecycle. May occur once a year or so in an operational environment.	Only small chance of occurring in the lifetime of the strategy.	May well occur during the lifetime of the strategy.	Likely to happen at some point during the next one or two years.	"Clear and present danger", represented by this risk - will probably impact on this initiative - sooner rather than later.
Programme / Project	Extremely infrequent – unlikely to happen in a strategic environment or occur during a project or programmes lifecycle. May occur once a year or so in an operational environment.	Not likely to occur during the lifecycle of the programme of project.	May occur during the life of the programme or project.	Likely to happen in the life-cycle of the programme or project.	Likely to occur in the life-cycle of the project, probably early on and perhaps more than once.
Operational	Extremely infrequent – unlikely to happen in a strategic environment or occur during a project or programmes lifecycle. May occur once a year or so in an operational environment.	Does not happen often - once every six months.	May well happen on a monthly basis.	May well happen on a weekly basis.	The threat is likely to happen almost every day.

RISK MATRIX DEFINITIONS

IMPACT TYPES

IMPACT

Public Protection	Financial	Reputation
Catastrophic 5	**Catastrophic 5**	**Catastrophic 5**
A systematic failure for which HCPC are ultimately responsible for, exposes the public to serious harm in cases where mitigation was expected.	Unfunded pressures greater than £1 million	Incompetence/ maladministration or other event that will destroy public trust or a key relationship
Significant 4	**Significant 4**	**Significant 4**
A systematic failure for which HCPC are ultimately responsible for, exposes more than 10 people to harm in cases where mitigation was expected.	Unfunded pressures £250k - £1 million	Incompetence/ maladministration that will undermine public trust or a key relationship for a sustained period or at a critical moment.
Moderate 3	**Moderate 3**	**Moderate 3**
A systemic failure for which HCPC are ultimately responsible for exposes more than 2 people to harm in cases when mitigation was expected.	Unfunded pressures £50,000 - £250,000	Incompetence/ maladministration that will undermine public trust or a key relationship for a short period. Example Policy U-turn
Minor 2	**Minor 2**	**Minor 2**
A systemic failure which results in inadequate protection for individuals/individual communities, including failure to resolve celebrity cases.	Unfunded pressures between £20,000-£50,000	Event that will lead to widespread public criticism.
Insignificant 1	**Insignificant 1**	**Insignificant 1**
A systemic failure for which fails to address an operational requirement	Unfunded pressures over £10,000	Event that will lead to public criticism by external stakeholders as anticipated.

LIKELIHOOD AREAS

LIKELIHOOD

Strategic	Programme / Project	Operational
Probable 5	**Probable 5**	**Probable 5**
"Clear and present danger", represented by this risk - will probably impact on this initiative - sooner rather than later.	Likely to occur in the life-cycle of the project, probably early on and perhaps more than once.	The threat is likely to happen almost every day.
Possible 4	**Possible 4**	**Possible 4**
Likely to happen at some point during the next one or two years.	Likely to happen in the life-cycle of the programme or project.	May well happen on a weekly basis.
Unlikely 3	**Unlikely 3**	**Unlikely 3**
May well occur during the lifetime of the strategy.	May occur during the life of the programme or project.	May well happen on a monthly basis.
Rare 2	**Rare 2**	**Rare 2**
Only small chance of occurring in the lifetime of the strategy.	Not likely to occur during the lifecycle of the programme of project.	Does not happen often - once every six months.
Negligible1	**Negligible1**	**Negligible1**
Extremely infrequent – unlikely to happen in a strategic environment or occur during a project or programmes lifecycle. May occur once a year or so in an operational environment.	Extremely infrequent – unlikely to happen in a strategic environment or occur during a project or programmes lifecycle. May occur once a year or so in an operational environment.	Extremely infrequent – unlikely to happen in a strategic environment or occur during a project or programmes lifecycle. May occur once a year or so in an operational environment.

HCPC Strategic Objectives 2016 - 2020

code	
SO1.GG	**Objective 1: Good governance** **To maintain, review and develop good corporate governance** Specific risks; 4.1 to 4.17 inclusive
SO2.EBP	**Objective 2: Efficient business processes** **To maintain, review and develop efficient business processes throughout the organisation** Specific risks; 1.1; 1.2; 1.2; 2.3; 4.1; 4.5; 4.6; 4.7; 4.12; 9.2
SO3.Com	**Objective 3: Communication** **To increase understanding and awareness of regulation amongst all stakeholders** Specific risks; 3.1; 3.2; 3.3; 3.4; 3.5
SO4.Evid	**Objective 4: Build the evidence base of regulation** **To ensure that the organisation's work is evidence based** Specific risks; 14.2
SO5.IPA	**Objective 5: Influence the policy agenda** **To be proactive in influencing the wider regulatory policy agenda** Specific risks; 1.2; 1.5
SO6.HmCty	**Objective 6: Engagement in the four countries** **To ensure that our approach to regulation takes account of differences between the four countries** Specific risks;

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

a. Identify all relevant risks
b. Mitigate those risks to an appropriate level
c. Invest mitigation resources in proportion to the level of risk

HCPC Risk Assurance mapping

Increasing Assurance →

	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		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			