

Audit Committee, 8th September 2015

Risk Register & Risk Treatment Plan

Executive summary and recommendations

Introduction

1. The Risk Register and Risk Treatment plan is a document reflecting current and recent levels of risk recognised by risk owners, who are the executive and Chair of Council.
2. The Risk Register and Risk Treatment plan is updated every six months, and changes are suggested by risk owners. Changes can be proposed outside of the review cycle, should the regulation environment or risk landscape change.
3. The changes are agreed at monthly EMT meetings. Residual risk is implicitly accepted for any current risk register.
4. The latest iteration of the risk register is presented here following updates gathered over the summer with face to face meetings with risk owners.

Decision

The Audit Committee is requested discuss the document.

Background information

None

Resource implications

None

Financial implications

None

Appendices

None

Date of paper

26th August 2015

1. Human resources

No changes to BPI resources.

2. Quality Management System (QMS) review meetings, internal audits and Near Miss Reports (NMR).

The internal audit schedule for 2015 – 16 is running.

One external audit was cancelled due to internal resource pressures around NMR55 and associated auditing. This mine Archive audit will be rescheduled for October / November.

NMR's

Three NMR's are under investigation at present;

NMR53 Education details on website not displayed in full (work around in place)

NMR54 Lapsed suspension orders in FTP

NMR55 Redaction quality in FTP bundles.

3. QMS process updates

The migration of the Quality Management System (QMS) to an externally hosted system has been terminated. The new access model following an upgrade to the hosting platform was found to be incompatible with our click through access requirement. We will therefore be planning to migrate our QMS & ISMS to a hosted MS SharePoint environment over the autumn. Experimentation with various "Add-ins" to support the required functionality is underway.

4. BSI audit

The next ISO9001:2008 two day audit will take place on 22nd & 23rd October.

Overview: Quality Management System Processes; Work Environment & Infrastructure; Projects; Registrations CPD, Operations, Quality Assurance; IT Infrastructure, Service Support ; Secretariat, Customer Services, Information Governance, Council processes.

5. Business continuity

Work on the layout and functionality of the Shadow Planner solution is underway. A test upload of Employee data to the system has taken place. Content of the plan is being reformatted to allow display on the Shadow Planner mobile platform.

6. Information security management

Information Security awareness activities continue around HCPC. These include updated mouse mats, and coasters with key information security messages. These were designed to ensure employees are fully aware of the requirements to achieve ISO27001 certification.

ISO27001 certification was officially achieved on 12th June 2015, and Kayleigh & I will be attending BSI Milton Keynes for the official presentation.

An unannounced Tidy Desk audit was carried out on parts of 33 Stannary Street on Friday 21 August. All areas audited were found to be compliant. No PII was found unprotected.

The next Continuing Assessment Visit is due for April 13-14th 2016

7. Information & data management

Assessment and destruction of older archive material: an update on progress.

The Registration department hope to progress the destruction of scanned renewal notices as soon as the archive boxes can be validated as “renewals”. A pre destruction visit to the archive is being planned.

Work with the Registrations department on sites for secure scanning continues prior to tests with internal CPD processes.

8. Reporting

The number of Freedom of Information requests of a statistical nature is currently static.

9. Risk Register

The latest iteration (Sept 2015) is published here following updates over the summer. The next iteration will be based on updates collected over December and January, with publication due for March.

Items of interest include, closure of the Risk around unknown structure of the PSA fee formula – this is now known, but replacement with a new risk around unexpected changes to fees per registrant.

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
20150605	a	QUA	RPT	AuditComm	Draft DD: None	Public RD: None

Risk Register & Risk Treatment Plan

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



July 2015 Risk Assessment

Contents	Page
Contents page	6
Top 10 HCPC risks	7
Changes since last published	8
Strategic risks	9
Operations risks	10
Communications risks	11
Corporate Governance risks	12
Information Technology risks	13
Partner risks	14
Education risks	15
Project Management risks	16
Quality Management risks	17
Registration risks	18
HR risks	19
Legal risks	20
Fitness to Practise risks	21
Policy & Standards risks	22
Finance risks	23
Pensions risks	25
Information Security risks	26
Appendix i Glossary and Abbreviations	27
Appendix ii HCPC Risk Matrix	28
HCPC Risk Matrix terms detail	29
Appendix iii HCPC Strategic Objectives & Risk Appetite	30
Appendix iv HCPC Assurance Mapping	31

THE HEALTH AND CARE PROFESSIONS COUNCIL

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

Historic Risk Scores

ID	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Mitigation I	Mitigation II	Mitigation III	CURRENT RISK SCORE	Feb 2015 Risk	Sept 2014 Risk	Feb 2014 Risk	Sept 2013 Risk	Feb 2013 Risk	Sept 2012 Risk	Feb 2012 Risk	July 2011 Risk	Feb 2011 Risk	Sept 2010 Risk	Feb 2010 Risk	
2.7	Interruption to electricity supply (pre-mit 16) ISMS RISK	Facilities Manager	Relocate to other buildings on site	If site wide longer than 24 hours invoke DR Plan	-	High	High	High	High	High	High	High	High	High	High	High	High	High
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	High	High	High	High	High	High	High	High
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												
2.11	Basement flooding (pre-mit 16)	Facilities Manager	Flood barrier protection to prevent ingress	-	-	Medium	Medium	Medium	Medium	Medium	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								
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	Medium	Medium	Medium	Medium	Medium
12.1	Judicial review of HCPC's implementation 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	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												

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
All	All	Update all dates to latest iteration of risk register	
Strategic Risks	1.1	Add Mitigation III	Ensure Strategic Intent is up to date.
	1.5	Lower likelihood 4 > 3	Lowers Risk
Communications	3.3	Update Mitigations I & II	Disaster Recovery > Business Continuity
	3.5	Update Mitigation II & Mitigation III	Add ISO9001 and Forward Comms Planner
Corporate Governance	4.2	Lower likelihood 4 > 3	Lowers risk of conflict of interest with smaller Council
	4.3	Update Mitigation III	Edit mitigation
	4.10	Update description, Mitigation I & Mitigation III	
	4.12	Update Mitigation II & Mitigation III	
	4.15	Update Mitigation II & Mitigation III	
Partners	6.2	Update Description, Mitigation I	
	6.4	Update Description	
	6.5	Add to Description & update Mitigations I & II & III	Make Description more clear, and disirate from 6.2 Description
	6.6	Update Mitigation III	
	6.7	Update Mitigation III	
Education	7.2	Update Description, Mitigation II & Mitigation III	
	7.5	Update Mitigation II & Mitigation III	Reflects new Education IT system
	7.7	New risk around Monitoring processes	
Projects	8.18	Registration process review project - closed	Project closed
	8.2	Failure to successfully replace the Lotus Notes system with Microsoft Outlook	Project closed
Registrations	10.1	Update Mitigation III	Edit mitigation
	10.3	Update Mitigation III	Edit mitigation
	10.4	Update Mitigation III	Edit mitigation
HR	11.1	Update Mitigation I & III	
	11.2	Increase Likelihood 2 > 3, update Mitigation III	Risk increased
	11.3	Increase Impact & Likelihood 2 > 3, update Mitigation I	Risk increased
	11.4	Update Description, lower Likelihood 3 > 2, update Mitigation I & II	Risk lowered
	11.6	Lower Likelihood 3 > 2	Risk lowered
	11.7	Update Mitigations II & III	
	11.9	Lower Impact 5 > 4, update Mitigation I & III	Risk lowered
FTP	13.9	Add Mitigation III	New mitigation detail
Finance	15.23	PSA Fee model risk removed	Fee structure now known
	15.25	Lower likelihood 3 > 2, update Mitigation I	Add Framework agreements to Mit I, old Mit I added to Mit II
	15.28	New PSA Fees risk, ongoing risk	Risk around fee per registrant inflation
Pensions	16.3	Lower Likelihood 2 > 1	Overall risk lowered as retirees crystallise lower outstanding benefits
Information Security	17.1	Add to Mitigations II & III	Include ISO27001
	17.3	Add to Description & update Mitigations II & III	Include ISO27001
	17.8	Add to Description & update Mitigations II & III	Include ISO27001
	17.19	Loss of ISO27001 certification	Add new risk post certification recommendation

Overview of Risk Management and Risk Treatment process

Throughout the year existing 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.

THE HEALTH AND CARE PROFESSIONS COUNCIL
 RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

Strategic

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

THE HEALTH AND CARE PROFESSIONS COUNCIL
RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

Operations

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
2	Operations	I	2.1	Inability to occupy premises or use interior equipment	Facilities Manager	4	3	12	Invoke Disaster Recovery/Business Continuity plan	Commercial combined insurance cover (fire, contents, terrorism etc)	-	Low	Low
	Operations		2.2	Rapid increase in registrant numbers Links to 1.2, 13.4	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
	Operations		2.3	Unacceptable service standards Links to 9.1, 10.4	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
	Operations		2.4	Inability to communicate via postal services (e.g. Postal strikes)	Facilities Manager	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	Facilities Manager & 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	2.6	Inability to accommodate HCPC employees Links to 5.2	Facilities Manager	4	3	12	Ongoing Space planning	Additional premises purchase or rented	-	Low	Low
	Operations	I	2.7	Interruption to electricity supply	Facilities Manager	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	Facilities Manager	1	2	2	Temporary heaters to impacted areas	-	-	Low	Low
	Operations		2.9	Interruption to water supply	Facilities Manager	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	2.11	Basement flooding	Facilities Manager	4	4	16	Flood barrier protection to prevent ingress	-	-	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 (formerly 11.5)	Health & Safety of employees Links to 4.9, 6.3	Chief Executive & Facilities Manager	5	4	20	Health & Safety Training, policies and procedures	H&S Assessments	Personal Injury & Travel insurance	Low	Low
	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 Jul 2015

Communications

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
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 advertising, 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
	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, Professional 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

THE HEALTH AND CARE PROFESSIONS COUNCIL
RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

Corporate Governance

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
4	Corporate Governance		4.1	Council inability to make decisions Links to 4.4	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	Attendance by external professionals as required	Low	Low
	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 Links to 4.1	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 including confirmation of attendance		Low	Low
	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	-	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? Links to 6.3	Director of Council & Committee Services , Facilities Manager & Finance Director	4	2	8	Safety briefing at start of each Council or Committee meeting.	H&S information on Council Extranet	Personal Injury and Travel insurance	Low	Low
	Corporate Governance		4.10	Establishing appropriately constituted Council Links to 6.1, 11.13	Chair	4	2	8	Robust and effective recruitment process	Use of skills matrix in recruitment exercise	Induction of Council members	Low	Low
	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 Extranet and made clear during induction	Budget holder review and authorisation procedures	Low	Low
	Corporate Governance		4.12	Operationalise Section 60 legislation	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	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	PSA informed of any deviations from agreed process at earliest opportunity	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 Jul 2015

Information Technology

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
5	IT	I	5.1	Software Virus damage <small>Links to 2.3, 10.2</small>	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
	IT	I	5.2	Technology obsolescence, (Hard/SoftWare) <small>Links to 2.6, 10.2</small>	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
	IT	I	5.3	Fraud committed through IT services <small>Links to 10.2 and 17.1</small>	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
	IT	I	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	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	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 2015

Partners

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
6	Partners		6.1	Inability to recruit and retain suitable Partners Links to 4.10, 11.3, 7.3,	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
	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 Links to 4.9	Partner Manager	3	2	6	H&S briefing at start of any HCPC sponsored event.	Liability Insurance	-	Low	Low
	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 notification 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 Jul 2015

Education

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
7	Education		7.1	Failure to detect low education providers standards Links to 1.1, 4.3, 6.4	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
	Education		7.2	Education providers disengaging with process Links to 1.1	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
	Education		7.3	Inability to conduct visits and monitoring tasks Links to 1.1, 6.1, 11.2 & 11.3	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
	Education		7.4	Loss of support from Education Providers Links to 1.1, 14.2	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
	Education	I	7.5	Protracted service outage following Education system failure	Director of IT	3	2	6	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	2	6	Operational processes (approval, monitoring and complaints about an approved programme)	Partnerships with Visitors and professional groups.	Regular training of employees and visitors	Low	Low
	Education	NEW	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 Jul 2015

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 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
8	Project Management		8.1	Fee change processes not operational by required date Links to 1.1, 15.3	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
	Project Management		8.2	Failure to regulate a new profession or a post-registration qualification as stipulated by legislation Links to 1.1, 15.3	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
	Project Management		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		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	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
	NEW Project Management		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	NEW

THE HEALTH AND CARE PROFESSIONS COUNCIL
 RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

Quality Management

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
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	9.2	Employees non-compliance with established Standard Operating Procedures	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 2015

Registrations

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
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	CPD		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 regulator feedback to the Education & Training Committee	Low	Low
				Links to 1.1									

THE HEALTH AND CARE PROFESSIONS COUNCIL
RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

HR

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
11	HR		11.1	Loss of key HCPC employees	Chair, Chief Executive and EMT	3	2	6	Organisation succession plan held by Chief Executive and HR Director.	Departmental training (partial or full) and process documentation	Informal department level succession plans	Low	Low
	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
	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 progress reviews	Low	Low
	HR		11.7	Employee and ex-employee litigation	HR Director	4	3	12	Regular one to one sessions between manager and employee and regular performance reviews.	Keeping HR policies and processes in line with employment legislation	Employee surveys, Exit Interviews, Employee Assistance Programme, Management Development Programme.	Low	Low
	HR	I	11.8	Employer/employee inappropriate behaviour	HR Director	2	2	4	Whistle blowing policy, Code of Conduct & Behaviour	Other HR policies and procedures	Employee Assistance programme	Low	Low
				Links to 11.3									
	HR		11.9	Non-compliance with Employment legislation	HR Director	4	2	8	Up to date HR policies and processes in line with employment legislation.	Obtain legislation updates and legal advice	HR training for managers	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL
 RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

Legal

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
12	Legal		12.1	Judicial review of HCPC's implementation of HSWPO including Rules, Standards & Guidance Links to 1.2, 14.1, 14.2	Chief Executive	5	3	15	Consultation. Stds determined by PLG's. Agreement by Council.	Appropriate legal advice sought	-	Medium	Medium
	Legal	I	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 implementation of the HSWPO	-	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL
 RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

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 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
13	Fitness to Practise		13.1	Legal cost over-runs Links to 13.4, 15.2	FTP Director	4	4	16	Contractual and SLA arrangements with legal services providers(s)	Quality of operational procedures	Quality assurance mechanisms	Low	Low
	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 Links to 13.1	FTP Director	4	4	16	Accurate and realistic budgeting	Resource planning	-	Medium	Medium
	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
	Fitness to Practise		13.7	High Number of Registration Appeals	FTP Director & Director of Operations, Head of Registrations	3	5	15	Training and selection of Registration Assessors, so reasoned decisions are generated	Quality of operational processes	-	Low	Low
	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 13.2 moved to 12.2	FTP Director	3	4	12	Reforecasting budget processes	Monthly management reporting	Resource planning & Quality of operational processes	Low	Low
	Fitness to Practise	I	13.10	Protracted service outage following a Case Management System failure	Director of IT	5	3	15	Effective backup and recovery procedures	Maintenance and support contracts for core system elements	Annual IT continuity tests	Low	Low

THE HEALTH AND CARE PROFESSIONS COUNCIL
 RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

Policy & Standards

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
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 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 government 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 Jul 2015

Finance

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
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	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	15.12	Unauthorised removal of assets (custody issue)	Facilities Manager & 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	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	Signed disclosure forms indicating tax category status for all Council and Committee members. Professional tax advice sought where necessary, including status of CCM's 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

THE HEALTH AND CARE PROFESSIONS COUNCIL
 RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

Finance

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
	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
	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	New

THE HEALTH AND CARE PROFESSIONS COUNCIL
 RISK ASSESSMENT & RISK TREATMENT PLAN Jul 2015

Pensions

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
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 Jul 2015

Information Security

Ref	Category	ISMS Risks	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2015	Likelihood before mitigations Jul 2015	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2015	RISK score after Mitigation Jan 2015
17	Information Security	I	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	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	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	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	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	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	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
	NEW Information Security	I	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
	NEW Information Security	I	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	New

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 occurring. 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 statutory 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

Appendix ii

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

>11 High Risk: Urgent action required

6-10 Medium Risk: Some action required

<5 Low Risk: Ongoing monitoring required

RISK MATRIX DEFINITIONS

IMPACT TYPES

	Public Protection	Financial	Reputation
IMPACT	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 greater than £50,000 £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 greater than £8,000 £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 over £2,000 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 £1,000 Unfunded pressures over £10,000	Event that will lead to public criticism by external stakeholders as anticipated.	

LIKELIHOOD AREAS

	Strategic	Programme / Project	Operational
LIKELIHOOD	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 2009 - 2015

code

SO1.GG	Objective 1: Good governance To maintain, review and develop good corporate governance
SO2.EBP	Objective 2: Efficient business processes To maintain, review and develop efficient business processes throughout the organisation
SO3.Com	Objective 3: Communication To increase understanding and awareness of regulation amongst all stakeholders
SO4.Evid	Objective 4: Build the evidence base of regulation To ensure that the organisation's work is evidence based
SO5.IPA	Objective 5: Influence the policy agenda To be proactive in influencing the wider regulatory policy agenda
SO6.HmCty	Objective 6: Engagement in the four countries To ensure that our approach to regulation takes account of differences between the four countries

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

HPCPC Risk Assurance mapping

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