Audit & Risk Assurance Committee

16 September 2021

HCPC Operational Risk Management

Executive Summary

The HCPC's Operational Risk Management process and register has been reviewed and updated and launched in Q1 of 2021-22. The review utilised the expertise of an external risk management consultant and took a bottom-up approach through dedicated departmental wide ranging risk discussions through a workshop.

This review resulted in a more concise operational risk register focused on the key areas of concern articulated by the risk owners. All operational risks have been mapped to the strategic risks they sit under. We have also introduced a risk management policy, guide and one pager quick guide for users for the first time.

The review and new approach to operational risk has been audited by BDO, and is the subject of a further paper at this meeting. The results were largely positive and provide assurance that the new approach is suitable for the HCPC's needs.

Previous consideration	Policy and guidance around operational risk, and the operational risk register have been considered by ELT. Plans for the operational review have been discussed with ARAC at previous meetings.
Decision	The Committee is asked to consider how it wishes to engage with operational risk in the future and future reporting needs.
Next steps	Ongoing quarterly discussions and updates from risk owners, and publication to ELT.
Strategic priority	SR5. Build a resilient, healthy, capable and sustainable organisation
Risk	This paper updates ARAC on the changes implemented with the operational risk register. It is relevant to all strategic risks.
Financial and resource implications	No direct costs associated with this updated process. The costs of the review were included in the 2020-21 budget.
Author	Roy Dunn, Chief Information Security & Risk Officer roy.dunn@hcpc-uk.org

HCPC Operational Risk Management

1. Introduction

The HCPC has undertaken a project to launch a new approach to risk management. Part one consisted of a rearticulation of our risk appetite and our Strategic Risks. Part two has involved redesigning our operational risk management processes and register with the aim of a more user friendly, concise and relevant register with greater risk ownership from risk owners.

2. Approach

The project lead the Chief Information Security and Risk Officer was supported in running the project by an independent risk management consultant who provided challenge and support.

The Operational Risk Register was built from the bottom up through the articulation of the risk owners. Workshops were held with Risk owning teams, which were welcomed by those involved. The process included;

- Risk Identification
- Risk Analysis and Evaluation
- Risk Treatment
- Risk Reporting & Monitoring

There was an overall aim to reduce the number of risks to those most relevant and requiring monitoring, simplify the process, and ensure the risk owners felt ownership of their risks.

The register is attached to this paper at appendix A. Appendices B, C and D set out the Policy, Guidance and quick guide to accompany the new approach.

3. Operational risk register

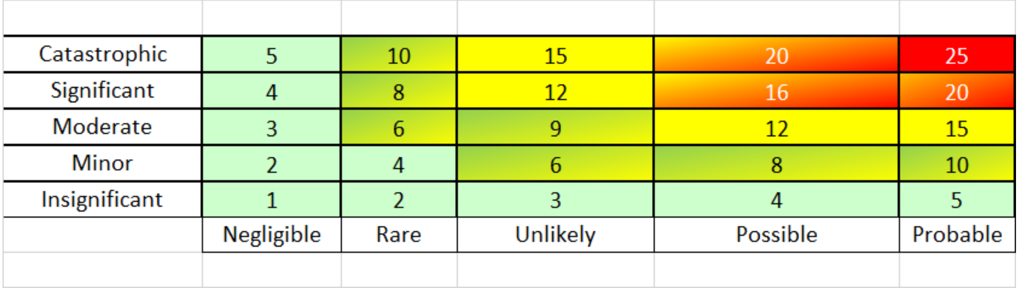
All risks have been articulated anew not based on the previous register, with a particular phraseology around the risk description, namely: Event – Cause – Consequence.

The first iteration of mitigation collection and scoring has taken place. We are now undergoing the second round of quarterly updates with operational risk owners. This will continue on a quarterly basis through 1:1 discussions with risk owners.

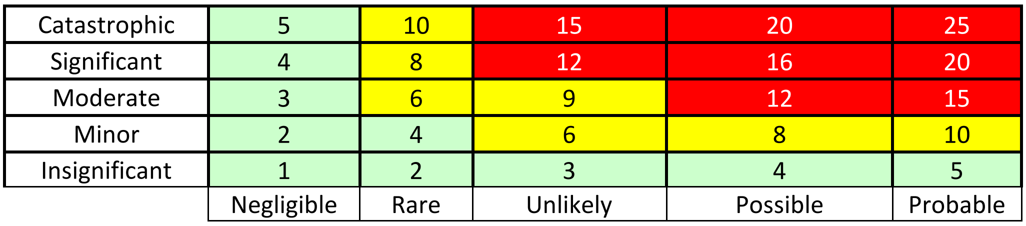
Following feedback from ELT, the level of detail (granularity) in the risk scoring regime has been increased, and this will likely be replicated in the Project Management risk process for new projects going forward. The new levels of risk are; Low, Low/Medium, Medium, Medium/High, High.

The Strategic Risk Register will not change from the existing Low, Medium and High rating system that is already in place.

The change in risk scoring is illustrated in the two graphics below. The first image is the new risk matrix with increased granularity with 5 risk levels. These differing levels are also compared visually in the last image.

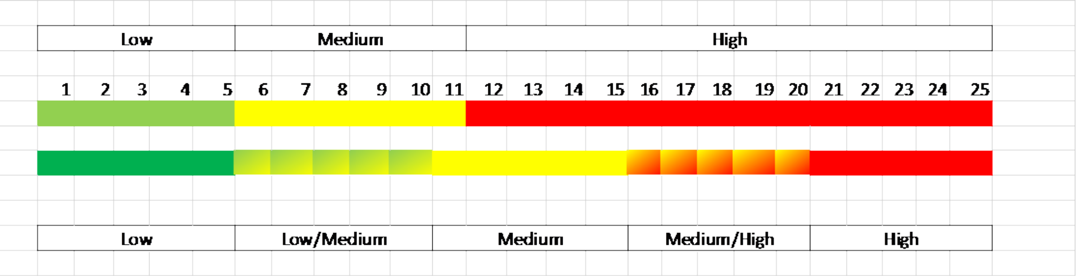


Catastrophic	5	10	15	20	25
Significant	4	8	12	16	20
Moderate	3	6	9	12	15
Minor	2	4	6	8	10
Insignificant	1	2	3	4	5
	Negligible	Rare	Unlikely	Possible	Probable



Catastrophic	5	10	15	20	25
Significant	4	8	12	16	20
Moderate	3	6	9	12	15
Minor	2	4	6	8	10
Insignificant	1	2	3	4	5
	Negligible	Rare	Unlikely	Possible	Probable

The two scales, old and new are further compared below.



4. BDO review

The HCPC's internal auditors BDO undertook a review of the HCPC's new approach to risk and the method used to formulate this. The results of this review are on the Committee's agenda at this meeting. The results are largely positive and provide assurance that a suitable system has been developed. The Executive will act on the recommendation that the Operational Risk management Guide and Policy be expanded to cover all aspects of risk management mainly the inclusion of Strategic and Project Risks.

5. Committee decision

This paper is for discussion with the Committee. A particular area of interest for the Executive is the Committee's future engagement with the Operation Risk Register and the frequency of this.

A possible approach is that the Committee receive the full register once a year with a commentary on changes/trends through the year of review.

Then at each meeting, when considering the thematic review of Strategic Risks, the Executive extract the operational risks that sit below a particular risk or theme and include this in the paper for reference to support the presenting lead's narrative.

6. Appendices

A- Operational Risk Register
B- Operational Risk Management Policy
C- Risk Management Gide
D- Quick user one page guide.

HCPC Operational Risk Register

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihooc	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
4	22	Strategy	Communications Strategy not Aligning with the Corporate Strategy	Communications not aligning with the corporate strategy will affect communications effectiveness.	Communications	Executive Director, Professional Practise and Insight	Moderate 3	Unlikely 3	12	Mitigate	Very regular touch points & engagement between those involved; Comms Team, Policy team, Exec, Luther & Chair. Luther stakeholder mapping completed Regular meetings between CER, Exec Dir & Luther	Exec Dir PPI	Ongoing ELT July 2021	Medium	Sept/Oct 2021	
4 5	23	Strategy	Communications Department Resourcing Limitations	Communications Department resourcing issues will impact communication quality and responsiveness which will mean Council and SMT requirements are not met due to the Communications Department not having the required staffing numbers or range of skills.	Communications	Executive Director, Professional Practise and Insight	Moderate 3	Possible 4	12	Mitigate	Team engagement Recruit to vacant posts. Changing roles could increase turnover, so support team throughout	Exec Dir PPI & Comms Team Lead	Oct-21	Medium/Low	Sept/Oct 2021	Generic risk more profound in Comms & Policy?
1 5 6	24	Operations	Digital Service Accessibility Issues	The rollout of the digitisation strategy for all interactions with registrants, partners and the public will impact service quality and stakeholder satisfaction due to specific stakeholder groups experiencing accessibility issues	Communications	Executive Director, Professional Practise and Insight	Minor 2	Unlikely 3	6	Mitigate	New Digital Officer post in place full-time to focus on user experience on website and supporting UX as digitisation strategy moves forward. Website hubs in place to support good UX - registrants, employers, education providers, students.	Comms Team Lead	Oct-21	Low	Sept/Oct 2021	
4	25	Reputation	Practise of Information and advice Issues	Inaccurate information and advice being provided to stakeholders will affect the reputation of HCPC due to the dynamic nature of the information and the multiple sources providing it.	Communications	Executive Director, Professional Practise and Insight	Minor 2	Possible 4	8	Mitigate	Processes in place for responding to policy queries. Regulat engagement between communications and policy teams and colleagues across the business to ensure responses are accurate. Plans to review sign off processes for policy responses and build bank of lines to take to support knowledge retention and transfer.	Head of Policy	Oct-21	Medium/Low	Sept/Oct 2021	Any PSA impact?

4	26	Reputation	Immature Reputational Communications Management	Inconsistent or inappropriate communications will impact the reputation of HCPC due to the processes for managing proactive, reputational communications being immature.	Communications	Executive Director, Professional Practise and Insight	Moderate 3	Unlikely 3	9	Mitigate	External Comms agancy in place to manage risk, Regular and close engagement between external agency, internal comms team and policy team. Forward plan aligned to strategy and shared weekly with CEO and Chair. CRM system when finances allow	Executive Director, Professional Practise and Insight	Oct-21	Medium	Sept/Oct 2021	Update target treatment dates as soon as possible
4	27	Reputation	Lack of Clarity of Communications Responsibilities	Duplicate, inconsistent or inappropriate communications will impact the reputation of HCPC due to a lack of clarity in the division of communications responsibilities between the Communications Department and other departments	Communications	Executive Director, Professional Practise and Insight	Minor 2	Unlikely 3	6	Mitigate	Communications team transitioning to Business Partner approach to ensure effective engagement across all departments. Communications team sole team responsible for sending out communications to registrants and employers; website and social media content.	Comms Team Lead	01-Jul-21	Medium/Low	Sept/Oct 2021	

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihood	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
1	32	Public Protection	Monitoring process failures	Low quality training being delivered by education providers will impact the reputation of HCPC, cause HCPC to be non-compliant to PSA standards and lead to public protection issues due to failures in monitoring processes	Education	Head of Education	Significant 4	Rare 2	8	Mitigate	1) Deliver monitoring processes which periodically check quality of programmes 2) Deliver processes in accordance with established KPIs 3) Embed quality checks within processes which ensure assessments are in line with standards.	Head of Education	Ongoing	Low	Sep-21	3 month review cycle
1	33	Public Protection	Approval process failures	Low quality training being delivered by education providers will impact the reputation of HCPC, cause HCPC to be non-compliant to PSA standards and lead to public protection issues due to failures in approval processes	Education	Head of Education	Significant 4	Rare 2	8	Mitigate	1) Deliver approval process which periodically check quality of programmes 2) Deliver processes in accordance with established KPIs 3) Embed quality checks within processes which ensure assessments are in line with standards.	Head of Education	Ongoing	Low	Sep-21	3 month review cycle
1 & 2	34	Operations	Lack of consistency in applying standards	Failure to achieve consistent outcomes across all education providers and professional areas will lead to training programmes achieving unjustified, different levels of compliance to standards due to the current approval and monitoring processes assessing education providers and professional areas in isolation of each other	Education	Head of Education	Insignificant 1	Possible 4	4	Mitigate	1) Deliver institution and programme level quality assurance processes which support greater consistency of outcomes across programmes. 2) Embed quality checks within processes which ensure assessments are in line with standards.	Head of Education	Ongoing	Low	Sep-21	3 month review cycle
1 & 5	35	Operations	Education Department resourcing Limitations	Education Department resourcing issues will impact service levels which will lead to statutory requirements for professional training delivery not being met and an inability to approve new training programmes due to the Education Department not having the required staffing numbers.	Education	Head of Education	Minor 2	Unlikely 3	6	Mitigate	1) Monitoring of case loads within QA processes 2) Effective forecasting of activity within budget cycles 3) Prioritisation of case progress where needed to ensure new programmes can achieve approval	Head of Education	Ongoing	Low	Sep-21	3 month review cycle
1 & 5	36	Operations	Inadequate visitor resourcing for smaller professional areas	Failure to deliver appropriate levels of service to smaller professional areas will lead to statutory requirements for professional training delivery not being met and an inability to approve new training programmes due to inadequate visitor resourcing for these professional areas	Education	Head of Education	Minor 2	Unlikely 3	6	Mitigate	1) Forecasting visitor requirements within budget cycles 2) Running recruitment campaigns which maximise applicant numbers for smaller professions.	Head of Education / Head of Partners	Ongoing	Low	Sep-21	3 month review cycle

5 INFO SEC	37	Information Security	Commercially Sensitive Data Breach	The confidentiality of commercially sensitive data being breached will impact the reputation of HCPC due to documentation being transferred to educational providers and visitors via unprotected email	Education	Head of Education	Minor 2	Rare 2	4	Mitigate	1) Use file encryption when sending assessment related documents to visitors 2) Use portal to manage secure document submission and access for visitors at case level for all assessments	Head of Education / Head of IT	Ongoing	Low	Sep-21	3 month review cycle

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihooc	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
5	1	Strategy	Leadership Consistency	Inconsistent leadership across the organisation will impact the delivery of key organisational objectives due to the lack of a defined leadership strategy and consistent leadership behaviours.	ELT	Chief Executive	Moderate 3	Possible 4	12	Mitigate	People strategy Corporate plans & dept workplans, Values & behaviours work across organisation.	Chief Executive	Nov-21	Low	Sept/Oct 2021	
4	2	Strategy	Relationship with Council	An ineffective relationship between the ELT and Council will lead to an inability to manage Council expectations due to a high rate of ELT churn and the relationship still evolving.	ELT	Chief Executive	Moderate 3	Possible 4	12	Mitigate	Corporate plan & strategy to ensure understanding, regular review of corporate plan deliverables to monitor progress.	Chief Executive	Nov-21	Low	Sept/Oct 2021	
5&6	3	Strategy	Poor Organisational Culture	Organisational culture issues will impact the delivery of key organisational objectives due to embedded siloed working, poor staff behaviours and a lack of accountability and ownership across the organisation.	ELT	Chief Executive	Moderate 3	Possible 4	12	Mitigate	Corporate plan & values, people strategy, establish broader leadership group ELT, SLT,etc	Chief Executive	Sep-21	Low	Sept/Oct 2021	
1&3&5&6	4	Strategy	High Rate of Change	Unsuccessful projects and initiatives will impact the delivery of key organisational objectives due to the rate of change across HCPC being too great for the organisation's capacity and capability.	ELT	Chief Executive	Moderate 3	Possible 4	12	Mitigate	Regular review of corporate plan delivery & prioritisation in light of resources availiable.	Chief Executive	Nov-21	Low	Sept/Oct 2021	
3&4	5	Strategy	External Relationship Management	Duplicate, inconsistent or inappropriate communications will impact HCPC's ability to influence the wider health environment due to poor management of external facing relationships and no central stakeholder management system.	ELT	Chief Executive	Minor 2	Possible 4	8	Mitigate	Monthly strategy & planning by ELT , incl horizon scanning, stakeholder engagement incl oversight by Luther	Chief Executive	In place	Low	Sept/Oct 2021	
5	6	Strategy	SMT Capacity Issues	ELT capacity issues will impact the delivery of organisational objectives due to the high rate of organisational change, high ELT churn and inadequate delegation.	ELT	Chief Executive	Minor 2	Possible 4	8	Mitigate	Establishing broader leadership group and heads of service roles as part of people strategy.	Chief Executive	Nov-21	Low	Sept/Oct 2021	
1&3&5&6	7	Strategy	Lack of Effective Horizon Scanning	An inability to predict future requirements will impact the effectiveness of business planning due to a lack of horizon scanning to identify emerging issues and opportunities.	ELT	Chief Executive	Minor 2	Possible 4	8	Mitigate	Monthly strategy & planning by ELT , incl horizon scanning, stakeholder engagement incl oversight by Luther	Chief Executive	Sep-21	Low	Sept/Oct 2021	
5	8	Strategy	Lack of Succession Planning	Single points of failure and inadequate corporate memory will affect organisational resilience due to weaknesses in succession planning, knowledge sharing and process documentation.	ELT	Chief Executive	Minor 2	Possible 4	8	Mitigate	Address single points of failure in organisational design, handover periods between interim & permanent positions wherever possible.	Chief Executive	Sep-21	Low	Sept/Oct 2021	Low to medium currently
5	9	Finance	Programme Overspend	Programme budget limits being exceeded will impact the delivery of organisational objectives and change due to a lack of clear programme prioritisation.	ELT	Chief Executive	Moderate 3	Unlikely 3	9	Mitigate	Corporate plan and deliverable tracking monitoring of budget spend	Chief Executive	Sep-21	Low	Sept/Oct 2021	

1 2 4 5 6	10	Operations	Failure to Deliver BAU Functions	BAU functions being insufficiently planned, resourced or managed will result in service failures and impact the reputation of HCPC with possible regulatory action due to a lack of departmental work plans, forecasting and performance monitoring.	ELT	Chief Executive	Significant 4	Possible 4	16	Mitigate	Dept workplans, monthy performance monitoring of BAU by ELT incl financial performance.	Chief Executive	Sep-21	Low	Sept/Oct 2021	

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihooc	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
5	11	Finance	Income System Failures	Process failures and accounting errors will impact the service delivered to registrants and lead to financial losses due to the new Income System not meeting business requirements and requiring multiple manual supporting processes.	Finance and Procurement	Director of Finance	Significant 4	Probable 5	20	Mitigate	Gordon Dixon re-engaged to develop plan as the first step	Gordon Dixon		Low	Sept/Oct 2021	
5	12	Finance	Poor Finance Process Documentation	Process failures and accounting errors will impact the service delivered to registrants and lead to financial losses due to current finance processes not being fully documented and there being an over-reliance on specific staff's process knowledge.	Finance and Procurement	Director of Finance	Significant 4	Probable 5	20	Mitigate	Gordon Dixon re-engaged to develop plan as the first step	Gordon Dixon		Low	Sept/Oct 2021	
5	13	Finance	Finance Department Resourcing Limitations	Process failures and accounting errors will impact the service delivered to registrants and lead to financial losses due to there being too few permanent staff to operate finance processes effectively and a reliance on temporary staff who do not have sufficient process knowledge.	Finance and Procurement	Director of Finance	Significant 4	Probable 5	20	Mitigate	Gordon Dixon re-engaged to develop plan as the first step	Gordon Dixon		Low	Sept/Oct 2021	
5	14	Strategy	Operational Improvement Delays	The Finance Team failing to expand their skills will affect the progress of operational improvements due to ongoing system, process and resourcing issues meaning the team has no time to undertake training.	Finance and Procurement	Director of Finance	Moderate 3	Probable 5	15	Mitigate	Gordon Dixon re-engaged to develop plan as the first step	Gordon Dixon		Low	Sept/Oct 2021	
5	15	Operations	Vendor Management Immaturity	Vendor contracts and agreements not fully meeting HCPC requirements will affect vendor service quality and HCPC vendor costs due to the immaturity of the vendor management processes.	Finance and Procurement	Director of Finance	Minor 2	Possible 4	8	Mitigate	Ongoing audit of new and existing contracts as they are renewed.	CISRO	Nov-21	Low	Sept/Oct 2021	As part of ISO27001

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihood	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
1	38	Operations	FTP Process Inefficiencies	Inefficiencies in the FTP process will affect the delivery of organisational objectives due to FTP being a large percentage of HCPC's spend and FTP volumes and costs increasing.	FTP	Head of Fitness to Practice	Moderate 3	Unlikely 3	9	Mitigate	1. FTP improvement programme	Head of Fitness to Practise	31/03/2022	Low	30/09/2021	
1	39	Operations	FTP Improvement Project Failure	Failure of the FTP Improvement Programme will impact the effectiveness of existing FTP processes and limit the capacity and capability to deliver ongoing FTP improvements due to the Programme being too complex or allocated budgets being exceeded.	FTP	Head of Fitness to Practice	Significant 4	Possible 4	16	Mitigate	1/ FTP improvement programme	Head of Fitness to Practice	31/12/2021	Medium	30/09/2021	
1	40	Public Protection	FTP Case Errors	A FTP case incorrectly not being progressed or proven will impact public protection and the reputation of HCPC due to FTP process failures or poor FTP decision making.	FTP	Head of Fitness to Practice	Significant 4	Rare 2	8	Mitigate	1/ FTP improvement programme 2/ Ongoing quality assurance activities	Head of Fitness to Practise	31/03/2022	Low	30/09/2021	
1 2 4	41	Public Protection	FTP Disputes	A FTP case being challenged by the PSA will impact public protection and the reputation of HCPC due to disagreements between the PSA and HCPC in how policies and standards should be applied.	FTP	Head of Fitness to Practice	Significant 4	Rare 2	8	Mitigate	1/ FTP improvement programme 2/ Ongoing quality assurance activities	Head of Fitness to Practise	31/03/2022	Medium	30/09/2021	Target risk rating remains medium due to ongoing possibility of PSA challenge and length of time it takes to see improvement on cases proceeding to final hearing
1 4	42	Public Protection	COVID-19 Impact	The FTP backlog becoming unsustainable will impact public protection and the reputation of HCPC due to COVID-19 restrictions preventing progress on cases that cannot be held remotely and department responsiveness being impacted by planning uncertainty.	FTP	Head of Fitness to Practice	Moderate 3	Unlikely 3	9	Mitigate	1/ FTP improvement programme 2/ Planning for return to in-person hearing activity to ensure options for hearing delivery remain open to us 3/ Seeking permanent Rules change to allow remote hearings	Head of Fitness to Practise	31/12/2021	Medium	30/09/2021	Target risk rating remains as medium due to ongoing uncertainty of the pandemic, and possibility of further restrictions in autumn/winter.
4&5 &6	56	Reputation	Ineffective Whistleblowing Processes (external issues)	Failure to identify and respond to issues will impact the reputation of HCPC and the level of service delivered to stakeholders due to ineffective external whistleblowing processes.	FTP	Head of FTP	Moderate 3	Unlikely 3	9	Mitigate	FTP standard response to raised concerns	Head of FTP	Current	Low	Sept/Oct 2021	Internal & externa whisletblowing split out

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihood	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
1&5 INFO SEC	43	Operations	Unclear Corporate Reporting Responsibilities	Ineffective corporate reporting will impact the reputation of HCPC and cause performance assessment issues due to reporting responsibilities not being clearly defined.	Governance	Head of Governance and Deputy Registrar	Minor 2	Possible 4	8	Mitigate	Monthly Dir reporting to SMT, redefined KPI's for Council, capability of analysis to be determined. Council & Committee reporting well defined.	Head of Governance and Deputy Registrar	Current	Medium	Sept/Oct 2021	
INFO SEC	44	Information Security	Information Security Policies Not Being Followed	Information security breaches will impact the confidentiality, integrity and availability of HCPC and stakeholder data due to staff not following information security policies for data handling, redaction and encryption.	Governance	Head of Governance and Deputy Registrar	Moderate 3	Possible 4	12	Mitigate	Reporting culture to see where not following requirements leads to incidents, and custom mitigations for specific areas.	CISRO / Head of Governance	Sep-21	Low	Sept/Oct 2021	
5 INFO SEC	45	Information Security	Poor Data Management by Suppliers	Poor data management by suppliers will impact the confidentiality, integrity and availability of HCPC and stakeholder data due to a lack of monitoring of supplier's compliance to HCPC data management policies.	Governance	Head of Governance and Deputy Registrar	Minor 2	Possible 4	8	Mitigate	Robust contracts and minimum certification requirements, to lower likelihood of breaches.	CISRO / Procurement	Sep-21	Low	Sept/Oct 2021	
1&2 &5	46	Operations	Legal Advice Access Issues	Issues with access to good quality and consistent legal advice will lead to incorrect and inconsistent decision making due to a reliance on external legal advice.	Governance	Head of Governance and Deputy Registrar	Moderate 3	Unlikely 3	9	Mitigate	Log all requests to ensure same scenarios are not investigaed? Two Co's on retainer, monthly contract mgmt	Head of Governance and Deputy Registrar	Current	Low	Sept/Oct 2021	
4	47	Strategy	Council Effectiveness	The quality of Council decision making will impact the ability of HCPC to plan and achieve its objectives due to the Council not receiving adequate information, not having time to review all options and not having the correct range of skills and training.	Governance	Head of Governance and Deputy Registrar	Moderate 3	Unlikely 3	9	Mitigate	Well researched papers, and guidenace of paper requirements, internal and external review. Skills matrix for members, gap analysis, regular Council seminars, policy issues, risk appetite	Head of Governance and Deputy Registrar	Current	Low	Sept/Oct 2021	
5 INFO SEC	48	Information Security	Lack of Information Security Awareness	Information security incidents will impact the confidentiality, integrity and availability of HCPC and stakeholder data due to a lack of information security awareness across all levels of the organisation.	Governance	Head of Governance and Deputy Registrar	Minor 2	Possible 4	8	Mitigate	Annual employee, Partner and temporary worker infosec training plus ongoing intranet/Teams messaging on current issues to heighten awareness	CISRO	Current	Low	Sept/Oct 2021	
1	49	Operations	Lack of Engagement with QA	Lack of engagement with the QA team will impact the level of compliance to team policies and processes due to the QA team's low profile and staff not understanding the benefits of the QA process.	Governance	Head of Governance and Deputy Registrar	Moderate 3	Unlikely 3	9	Mitigate	Ongoing engagement plan with Regulatory departments employees, SMT interaction. Internal Comms input, All employee mtg. Monthly Regulatory Mgr blog.	QA Lead	Current	Low	Sept/Oct 2021	
4	50	Reputation	Non-adherence to the Code of Corporate Governance	Lack of transparency and poor decision making will affect the reputation of HCPC due to Council members not adhering to the code of corporate governance	Governance	Head of Governance and Deputy Registrar	Moderate 3	Unlikely 3	9	Mitigate	External review by PSA annually, limited closed meetings based on preset criteria, regular training	Head of Governance and Deputy Registrar	Current	Low	Sept/Oct 2021	

4&5 &6	86	Reputation	Ineffective Whistleblowing Processes (internal)	Failure to identify and respond to issues will impact the reputation of HCPC and the level of service delivered to stakeholders due to ineffective internal whistleblowing processes.	Governance	Head of Governance and Deputy Registrar	Moderate 3	Unlikely 3	9	Mitigate	Promotion of internal whislteblowing process and annual training on anti-bribery and fraud	CISRO	Current	Low	Sept/Oct 2021	Internal & externa whisletblowing split out

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihooc	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
5	16	Finance	Enforced Partner Contract Changes	A requirement to convert partner contracts to employee contracts will lead to significant costs for HCPC due to changes in how employment law is interpreted and applied.	HR and Partner	Head of Human Resources	Significant 4	Probable 5	20	Mitigate	Create robust enforecable partner contracts which avoid employee/ worker status with the organisation.	Head of Partners	31.03.22	High	01.12.21	As contractors, not employees, training should not need to be significant.
1 & 5	17	Reputation	Ineffective Partner Training	An inability to provide effective partner training will affect partner performance, the reputation of HCPC and cause non-compliance to PSA standards due to difficulties in monitoring training effectiveness, ensuring it meets changing requirements and ensuring that partner's are fully engaged with it.	HR and Partner	Head of Human Resources	Moderate 3	Unlikely 3	9	Mitigate	Ongoing annual reviews with stakeholder input and aligned to the outcome of the tribunal case.	Head of Partners	31.03.22	Medium	01.12.21	Rqmt to provide less training to avoid employee status! RPD
5	18	Operations	Recruitment and Retention Issues	An inability to recruit and retain employees and partners will lead to higher training and churn costs and reduce the quality of service delivered by HCPC due to a competitive job market and a poor perception of HCPC amongst employees and partners.	HR and Partner	Head of Human Resources	Moderate 3	Possible 4	12	Mitigate	Develop a new People Strategy which has direct focus on developing the employer brand, recruitment strategies and retention.Focus on behaviours, aligning these through APDR and employee engagement	Head of Human Resources	30.09.21	Medium	31.08.21	
5	19	Operations	Limited Career Development Opportunities	Limited career development opportunities will affect employee churn rates and employee wellbeing and lead to single points of failure due to a lack of effective succession planning and unclear career paths.	HR and Partner	Head of Human Resources	Minor 2	Possible 4	8	Mitigate	Develop a new organisational Succession plan which focuses on career development opportunities.	Head of Human Resources	31.12.21	Medium	30.09.21	
5	20	Operations	Increased Flexible Working Requests	Requests for greater levels of flexible working by staff will have financial impacts on HCPC and make resource planning more complex due to all staff experiencing more flexible working arrangements during the COVID-19 pandemic.	HR and Partner	Head of Human Resources	Minor 2	Possible 4	8	Mitigate	Develop a New ways of working Policy in collaboration with Corporate Services	Head of Human Resources	31.03.22	Medium	01.12.21	
5	21	Operations	Staff Morale Issues	Low levels of employee morale will affect employee wellbeing and churn rates and reduce the level of service delivered by HCPC due to a poor perception of HCPC amongst employees and partners, a high level of organisational change and increasing job demands.	HR and Partner	Head of Human Resources	Minor 2	Possible 4	8	Mitigate	The new ways of working policy along with the introduction of an employee engagement strategy will enhance employee morale. For example, employees will be asked to particpate in identifying behaviuuors for all HCPC values.	Head of Human Resources	31.03.22	Medium	01.12.21	

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihood	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
5	51	Operations	IT Department Resourcing Limitations	IT Department resourcing issues will impact its ability to meet the requirements of an evolving HCPC organisation due to the IT Department not having the required staffing numbers or range of skills.	IT	Head of IT and Projects	Moderate 3	Possible 4	12	Mitigate	Prioritization of BAU and project work to maximise efficient use of resources available	Head of IT	Current	Low	Sept/Oct 2021	
5	52	Operations	Ineffective Recruitment Processes	Difficulties in recruiting appropriate staff in a timely manner will lead to ongoing resourcing issues due to the HCPC job application process being overly complex and not effectively selecting the right people to be interviewed.	IT	Head of IT and Projects	Minor 2	Possible 4	8	Mitigate	Eased recruitment process for some types of role as required	Head of IT / Head of HR	Current	Low	Sept/Oct 2021	
5 INFO SEC	53	Information Security	Successful Cyber Security Attacks	A successful cyber security attack will impact the confidentiality, integrity and availability of HCPC systems and data due to there being no dedicated technical security roles and no formal cyber security framework implemented to ensure the consistency and effectiveness of technical controls.	IT	Head of IT and Projects	Significant 4	Unlikely 3	12	Mitigate	Combination of ISO27001 & Cyber Essentials Plus to maintain minimal level of control as a baseline	Head of IT, Head of Governance	Current	Low	Sept/Oct 2021	
5 INFO SEC	54	Information Security	Inadequate Third Party Access Management	Third parties having inappropriate access to HCPC systems and data will affect the confidentiality of HCPC and stakeholder data due to the lack of effective processes for managing third party access.	IT	Head of IT and Projects	Moderate 3	Unlikely 3	9	Mitigate	Legal (contractural) and process requirements to gain access. (Includes ongoing oversight of work for some contractors, by infrastructure team)	Head of IT, Head of Governance	Current	Low	Sept/Oct 2021	
3 & 5 INFO SEC	55	Information Security	Lack of Data Management Processes	A lack of data management processes will affect the ability to share data efficiently and securely and lead to a risk adverse approach and multiple ad-hoc solutions due to a lack of clear data ownership, data classification and data handling guidelines.	IT	Head of IT and Projects	Minor 2	Possible 4	8	Mitigate	Use ISMS data ownership documentation to allow appropriate sign off as business requirements are fulfilled.	Head of IT, Head of Governance	Sep-21	Low	Sept/Oct 2021	

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihooc	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
5	80	Operations	Non-compliance to Fire Safety Regulations	Non compliance to fire safety regulations will increase the risk of a fire leading to a building being destroyed or being unavailable for a significant period of time due to buildings requiring a range of remedial work to achieve compliance to evolving fire safety regulations.	Office Services	Head of Estates and Facilities Management	Significant 4	Negligible 1	4	Mitigate	Service & Maintenance contracts in place for related systems and services; regular audit of H&S; employee training, building signage, monitored alarms systems,emergency lighting, regular fire evacuation tests (outside pandemic conditions). Leased premises, Landlord/Managing Agents organised evacuation tests and systems in place.Regular Managing Agent meetings.	Facilities Manager	Scheduled compliance testing, and systems already implemented	Low	Sept/Oct 2021	
5	81	Operations	Building Plant End of Life	Building plant failures and non compliance to standards will affect office availability and the quality of the office environment due to equipment such as boilers, air conditioning and lifts reaching end of life and requiring replacement.	Office Services	Head of Estates and Facilities Management	Moderate 3	Unlikely 3	9	Mitigate	Planned preventative maintenance contracts in place; reactive maintenance as required until funding for replacement plant is available.	Head of Estates and Facilities Management	PPM scheduled, Reactive beyond buget with SMT approval	Medium	Sept/Oct 2021	
5 INFO SEC	82	Operations	Failure of Server Room Power Supply	Failure of the power supply to the server room will impact the availability of IT systems due to the failover power supply only being tested once every 5 years.	Office Services	Head of Estates and Facilities Management	Moderate 3	Negligible 1	3	Mitigate	Diverse redundant power routing to main server room, with automated fail over. Minimum 5 year fixed power testing in place, UPS in place to allow elegant automated shut down of servers, aircon to server room on fail over power also.	Facilities Manager	In place.	Low	Sept/Oct 2021	
1 5 6	83	Operations	Inability to Process Post	Inability to process departmental post will affect the delivery of services to stakeholders due to HCPC offices not being accessible or equipment such as scanners not being available.	Office Services	Head of Estates and Facilities Management	Moderate 3	Rare 2	6	Mitigate	Franking machine replaced by leased equipment with support contract and maintenance, Postal credit card (held by Finance) to allow emergency manual processing in house. Potential reduction in post requirment long term as Digital first strategy delivers more services online.	Facilities Manager	In place, digital first strategy underway but difficult to proedict impact on postal requirement at present.	Low	Sept/Oct 2021	

5	84	Operations	Physical Security	Inability to provide adequate physical security for the protection of onsite individuals and organisational assets	Office Services	Head of Estates and Facilities Management	Significant 4	Possible 4	16		Physical and digital security systems and measures are in place supported by service, maintenance and monitoring contracts	Facilities Manager	In place, additional provisions or extensions of services will be made for any prevailing situation	Low	Sept/Oct 2021	
5	85	Operations	Health and Safety	non compliance with health and safety regulations increases risk of personal harm or injury	Office Services	Head of Estates and Facilities Management	Significant 4	Possible 4	16		Service & Maintenance contracts in place for related systems and services; regular audit of H&S; employee training, building signage, regular monitoring and planning for compliance with any adjustments to regulations	Facilities Manager	Scheduled compliance testing, and systems already implemented	Low	Sept/Oct 2021	

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihood	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
5	28	Operations	Policy and Standards Department Resourcing Limitations	Policy and Standards Department resourcing issues will impact its ability to meet the requirements of an evolving organisation and to be able to work proactively with the PSA rather than reactively due to the Department not having the required staffing numbers or range of skills and having multiple single points of failure.	Policy and Standards	Executive Director, Corporate Services	Moderate 3	Possible 4	12	Mitigate	Finance, recovery plan with addtn temp resource, Pol & Stds secondment, plus agreed budget for recruitment, prioristisation of elelements, some held back to accomodate resources	Chief Executive	Sep-21	Low	Sept/Oct 2021	
3 & 4	29	Operations	Lack of Intelligence Gathering and Analysis Processes	A lack of intelligence gathering and analysis will impact the reputation of HCPC due to appropriate expertise only recently being recruited and the associated processes still being developed.	Policy and Standards	Director, Digital Transformation	Moderate 3	Possible 4	12	Mitigate	Data Lake implementation deferred to 2022/23 FY	Head of IT	Jul-22	Low	Sept/Oct 2021	
3& 4	30	Reputation	EDI Non-Compliance	Failing to meet EDI goals will lead to regulatory non-compliances, inconsistencies in the level of service delivered to specific stakeholder groups and impact the reputation of HCPC due to ineffective EDI data collection processes.	Policy and Standards	Executive Director, Professional Practise and Insight	Moderate 3	Possible 4	12	Mitigate	1)Publication of registrant diversity data based on 18% of registrants 2)Recruit to EDI post contingant on agreement at July council 3)Digital team currently scoping out data collection process at registration. Considering also best approach to complainant data. 4)Rapid review of process against current strategy/plans to inform future activity and identify any further quick wins	Head of Policy Head of Policy Head of IT & Projects QA Team	July/Aug 2021 Sept/Oct 2021 2021/22? July - Aug 2021	Low	Sept/Oct 2021	
4 6	31	Strategy	Lack of Clarity on HCPC's Role	Registrants and their professional bodies being unclear of the role and responsibilities of HCPC will impact perceived service quality and the reputation of HCPC due to a lack of ongoing communication of HCPC objectives and responsibilities to stakeholder groups and changing HCPC business strategies.	Policy and Standards	Executive Director, Professional Practise and Insight	Minor 2	Possible 4	8	Mitigate	Ongoing standards review and communication of such Establishment of (1/4ly) professional body engagement group. Ongoing newslettrs, web content. Ongoing development of Professional Liaison function.	Head of Policy	Current First meeting July 2021	Medium	Sept/Oct 2021	

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihooc	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
5	70	Strategy	Absence of Annual Budget Planning	An absence of annual budget planning will impact the delivery of organisational objectives due to project roadmaps not aligning to the organisational strategy.	Project	Interim Head of IT and Projects	Minor 2	Possible 4	8	Mitigate	1/ Validate project roadmap alignment with organisation's strategy. 2/ Reintroduce portfolio planning processes.	Head of Projects		Low	Sept/Oct 2021	
5	71	Strategy	Project Department Resourcing Limitations	Project management resourcing issues will impact the delivery of organisational objectives due to the Project Department not having the required staffing numbers to deliver the high rate of required change.	Project	Interim Head of IT and Projects	Minor 2	Possible 4	8	Mitigate	1/ Work with Executive to agree an organisational level prioritisation process	Head of Projects		Low	Sept/Oct 2021	
5	72	Finance	Lack of an Integrated Financial System	Lack of an integrated financial system will result in inefficient management of project finances and discrepancies between project and finance accounting due to project financial management being a manual, stand alone process.	Project	Interim Head of IT and Projects	Minor 2	Unlikely 3	6	Mitigate	1/ Develop project finance processes that integrate with the new Finance system.	Head of Projects		Low	Sept/Oct 2021	
5	73	Finance	No Project Backfill Budgeting	Requirements to fund backfill on each project will result in higher than expected project spend due to there being no centralised allocation of budget for backfill requirements.	Project	Interim Head of IT and Projects	Minor 2	Possible 4	8	Mitigate	1/ Review options to create a centralised backfill budget for all change initiatives.	Head of Projects		Low	Sept/Oct 2021	
5&6	74	Strategy	Lack of Clear and Consistent Communication	A lack of clarity on the business strategy and its outcomes among employees will impact the delivery of organisational objectives due to a lack of clear and consistent communication from leadership.	Project	Interim Head of IT and Projects	Moderate 3	Possible 4	12	mitigate	Improve employee visability of project activity via internal communications?	Head of Projects		Low	Sept/Oct 2021	
5	75	Operations	Lack of Benefit Analysis and Tracking	A lack of benefit analysis and post implementation benefit tracking will result in poor project prioritisation and an unclear realisation of value due to a lack of measurable benefits being defined in each project business case and there being no clear business change ownership.	Project	Interim Head of IT and Projects	Minor 2	Possible 4	8	Mitigate	1/ Ensure all change initiative have an agreed business owner. 2/ Ensure measurable benefits are documented in all business cases.	Head of Projects	Sep-21	Low	Sept/Oct 2021	
5	76	Strategy	Ineffective Adoption of Agile Methodologies	Ineffective Agile methodology adoption will impact the delivery of organisational objectives due to a failure to fully assess the impact of Agile on existing processes and systems, poor staff awareness and a lack of training for key stakeholders.	Project	Interim Head of IT and Projects	Minor 2	Possible 4	8	Mitigate	1/ Create a training/mentoring plan for Agile. 2/ Implement plan.	Head of Projects	Sep-21	Low	Sept/Oct 2021	
5	77	Strategy	Project Governance Reduction	A reduction in project governance will impact the delivery of organisational objectives due to project initiation processes not being completed effectively when Agile methodologies are followed.	Project	Interim Head of IT and Projects	Minor 2	Unlikely 3	6	Mitigate	1/ Review project governance requirements with the Executive. 2/ Implement governance requirements.	Head of Projects		Low	Sept/Oct 2021	
5	78	Strategy	Poor Benefit Realisation	Poor benefits realisation will impact the delivery of organisational objectives due to projects and changes not being managed within a single strategy with a clear, prioritised roadmap.	Project	Interim Head of IT and Projects	Moderate 3	Possible 4	12	Mitigate	1/ Review project governance requirements with the Executive. 2/ Implement governance requirements within roadmap.	Head of Projects		Low	Sept/Oct 2021	

5	79	Strategy	Poor Supplier Service Levels	Poor service levels from suppliers will impact the delivery of organisational objectives due to a lack of ongoing supplier performance management.	Project	Interim Head of IT and Projects	Moderate 3	Possible 4	12	Mitigate	Ongoing monitoring of service supplied	Head of IT		Low	Sept/Oct 2021	

SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihood	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
1 & 2	57	Operations	Concentration on Remedial Work	Currently compliant professional areas may be developing underlying issues leading to future PSA non-compliances due to resource limitations meaning that areas not requiring remedial action have limited attention from the QA Department.	QA	QA Lead	Minor 2	Possible 4	8	Mitigate	QA activity in Regulatory departments. PSA working group monthly meetings.	QA Lead	Current	Low	Sept/Oct 2021	
1 & 5 & 6	58	Operations	Departments not complying with public facing standards and guidelines	Departments not complying with public facing standards and guidelines will lead to PSA non-compliances due to the QA Department having limited resources for compliance monitoring or cross-department collaboration and engagement.	QA	QA Lead	Minor 2	Possible 4	8	Mitigate	QA activity in Regulatory departments. PSA working group monthly meetings.	QA Lead	Current	Low	Sept/Oct 2021	

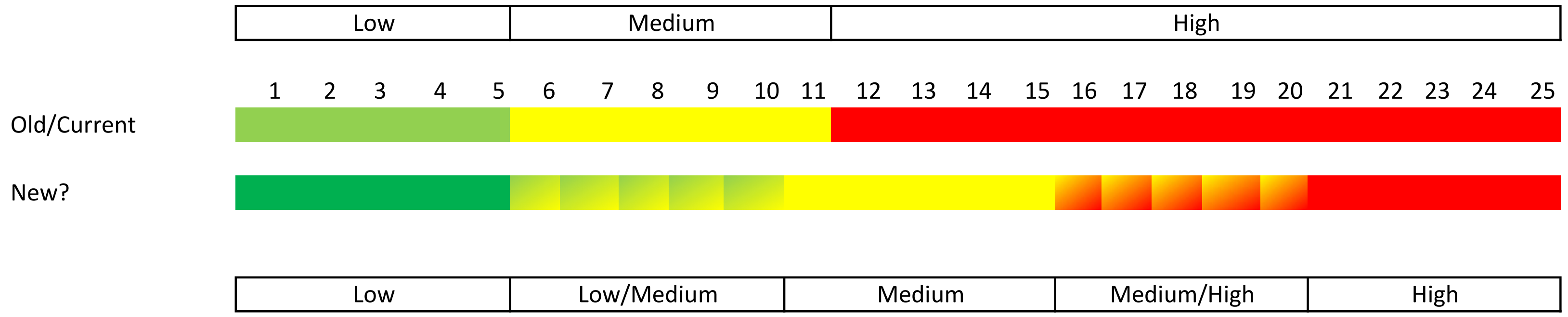
SR su	Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihood	Risk Rating L/LM/M/MH/H	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating L/M/H	Next Review Date	Risk Status Notes
1 & 4	59	Public Protection	Registration Process Failures	Public protection issues will lead to non-compliance to PSA standards and affect the reputation of HCPC due to staff errors in the registration process for new registrants.	Registration and CPD	Head of Registration	Significant 4	Rare 2	8	Mitigate	Audits by Registration Management, system audit trails, external auditors. Policy and procedures supported by ISO quality audits and process controls/checks	Head of Registration	Ongoing	Low	Sept/Oct 2021	
1 & 4	61	Public Protection	Registrant Fraud	Public protection issues will lead to non-compliance to PSA standards and affect the reputation of HCPC due to fraudulent information being used in registration or renewal applications.	Registration and CPD	Head of Registration	Significant 4	Negligible 1	4	Mitigate	Financial audits, system audit trails. Policy and procedures supported by internal quality audits.	Head of Registration	Ongoing	Low	Sept/Oct 2021	
1 & 5 & 6	62	Operations	System Failure	A technical failure of the online registration system will impact process registrations and renewals due to an increase in the use of the online application process.	Registration and CPD	Head of Registration	Significant 4	Possible 4	16	Mitigate	External IT support contracts. Well trained in house IT employees.Effective project management of new product delivery.	Head of Registration	Ongoing	Low	Sept/Oct 2021	
1 & 5	63	Operations	System Interfaces	A technical failure of any system that the registration team is reliant upon will impact registrations and renewals due to an increase in the number and complexity of interfaces between operational systems.	Registration and CPD	Head of Registration	Significant 4	Possible 4	16	Mitigate	External IT support contracts. Well trained in house IT employees.Effective project management of new product delivery.	Head of Registration	Ongoing	Low	Sept/Oct 2021	
5 INFOSEC	64	Information Security	Data Sharing	The confidentiality of data being breached will impact the reputation of HCPC due to registration and appeal data packs being transferred to external parties via unprotected email.	Registration and CPD	Head of Registration	Moderate 3	Unlikely 3	9	Mitigate	e-Bundles software to be tested and adopted if practical. Password delivery systems to be considered	Head of Registration	Ongoing	Low	Sept/Oct 2021	
1 & 5	65	Operations	Sustainability of Current Working Practices	Current COVID-19 work practices not being sustainable will impact staff availability and the ability to deliver registration services due to staff wellbeing being negatively impacted by factors such as high overtime rates.	Registration and CPD	Head of Registration	Minor 2	Possible 4	8	Mitigate	Regular contact with employees. Introduce hybrid working. HCPC Health and wellbeing initiatives.	Head of Registration	Ongoing	Low	Sept/Oct 2021	
4 5 6	66	Operations	Rollout of New Fee Structures	An increased likelihood of errors in the application of registrant fees will affect the reputation of HCPC and may lead to financial losses due to issues with the implementation of the new fee structure.	Registration and CPD	Head of Registration	Significant 4	Possible 4	16	Mitigate	Effective project management. Well documented processes.Financial audits and quality controls.	Head of Registration	Ongoing	Low	Sept/Oct 2021	
1 & 6	67	Operations	Appeal Process Regulation	The small pool of council members that are eligible to chair registration appeal hearings will impact the throughput of appeal cases and may cause the suitability of the chair to be challenged by appellants due to regulatory requirements being very restrictive on who can chair a registration appeal.	Registration and CPD	Head of Registration	Moderate 3	Unlikely 3	9	Mitigate	Recruit and train eligible council members.	Head of Registration	Ongoing	Low	Sept/Oct 2021	
1 & 6	68	Operations	Lack of Out of Hours Support	Failure to respond to online issues and questions outside of normal working hours will not meet registrants service level expectations due to the registration teams only being available during standard working hours.	Registration and CPD	Head of Registration	Minor 2	Unlikely 3	6	Mitigate	Clear guidance published on website. FAQs regularly updated on website. User experience testing before new product launch.	Head of Registration	Ongoing	Low	Sept/Oct 2021	

1 & 5	69	Operations	Insufficient Departmental Engagement in Projects	Insufficient departmental engagement in projects will result in business requirements not being fully met due to limitations on the amount of resource that departments can allocate to projects.	Registration and CPD	Head of Registration	Moderate 3	Possible 4	12	Mitigate	Dedicated resource included within project business case.	Head of Registration	Ongoing	Low	Sept/Oct 2021	

Collect updates	ELT meeting	Audit & Risk Comm
May		
June		
July	July	
August		
September		
October	October	
November		November
December		
January	January	
February		
March		
April	April	
May		
June		
July	July	

Impact	Likelihood	Rating	Treatment Type	Risk Category
Catastrophic	Probable	High	Mitigate	Finance
Significant	Possible	Medium	Accept	Information Security
Moderate	Unlikely	Low	Avoid	Strategy
Minor	Rare		Transfer	Operations
Insignificant	Negligible			Public Protection
				Reputation

Catastrophic	5	10	15	20	25
Significant	4	8	12	16	20
Moderate	3	6	9	12	15
Minor	2	4	6	8	10
Insignificant	1	2	3	4	5
	Negligible	Rare	Unlikely	Possible	Probable



Operational Risk Management Policy

1. Purpose

To maintain and improve the level of service HCPC delivers to its stakeholders, the organisation must understand and manage the risks it faces. Risks are inherent to HCPC activities and can relate to strategic threats, operational issues, reporting obligations and legal and contractual compliance. By understanding risk, HCPC has a foundation for effective decision making and prioritisation.

The purpose of this Operational Risk Management Policy (Policy) is to ensure that HCPC has a defined and consistent approach to managing operational risk. This will enable Heads of Departments to effectively identify, monitor and treat risk within their areas and will provide the HCPC Senior Management Team (SMT) with an accurate overview of the type and level of operational risk across the organisation.

2. Scope

This Policy applies to all teams and processes across HCPC involved in the identification, assessment and treatment of operational risk.

3. Policy Statements

Risk can be defined as “the effect of uncertainty on objectives”. It can be considered to be the potential harm that a given threat or exploitation of a vulnerability will cause to HCPC assets such as company reputation, information, processes, systems, equipment or buildings. Risk can also present opportunities and the impact of these on objectives should also be considered.

4. Risk Methodology and Approach

Within HCPC all operational risks will be managed via the Operational Risk Management (ORM) process. Heads of Departments will be responsible for utilising this process to identify and manage risks within their areas supported by the Chief Information Security & Risk Officer who will provide process oversight and coordination.

All operational risks will be recorded in the HCPC Operational Risk Register.

The SMT will be responsible for managing the Strategic Risk Register. Where applicable and with agreement from the HCPC SMT, operational risks from the Operational Risk Register may be:

- Escalated to the Strategic Risk Register.
- Linked to risks in the Strategic Risk Register.

The ORM process will:

- Be a proactive ongoing process.
- Ensure that all risks are documented in a consistent manner.
- Ensure that each risk has an associated treatment plan with agreed steps and timelines.
- Ensure each risk has a single risk owner.
- Ensure each risk is periodically revied to confirm its validity and to monitor treatment plan progress.

5. Risk Appetite

The Council is responsible for setting the HCPC risk appetite and periodically reviewing it to ensure that it continues to meet the needs of the organisation, The Council receives advice from the Audit and Risk Assurance Committee when making these decisions.

The risk appetite will be referenced when determining how risks will be treated

6. Risk Identification

Risks will be identified via a range of standard business activities such as incident management, audits and process monitoring as well as via specific risk management activities such as risk workshops.

Departmental managers are responsible for ensuring that potential risks are:

- Reviewed.
- Formally defined with a clear cause, event and consequence.
- Allocated to a risk owner with appropriate accountability and authority to manage the risk.

7. Risk Assessment and Measurement

During risk assessment, risk owners will ensure that the following are undertaken:

- Assessment of any relevant current controls and their effectiveness.
- Analysis of the likelihood of the risk occurring.
- Analysis of the consequences (impact) of the risk.

The risk rating will be determined by taking into account both the likelihood and the impact of the risk.

To ensure risks are assessed in a consistent manner across all HCPC departments, the SMT will approve HCPC risk likelihood and risk consequence tables. These tables will be used by risk owners to determine the risk rating of their risks.

8. Risk Response and Action

For all risks that are assessed to be above the HCPC risk appetite, the risk owner is responsible for ensuring that a treatment plan is developed that either mitigates, transfers or avoids the risk. The risk owner is also responsible for allocating risk treatment owners and monitoring their progress in delivering their actions.

Mitigating actions for risks must reduce the risk to an agreed target risk rating (i.e., the level of risk that will remain once the treatment plan is complete) within an agreed timescale.

9. Monitoring

Risk owners will monitor their allocated risk and risk treatment activities on a regular basis to ensure that their risks remain within acceptable levels.

The SMT will receive periodic risk updates from risk owners.

The Chief Information Security & Risk Officer will oversee the ORM process to ensure that all risks are being monitored and managed in line with the HCPC risk appetite.

10. Reporting

The Chief Information Security & Risk Officer will provide the SMT with periodic risk reports to enable it to fulfil its risk oversight role and to gain assurance that risks are being proactively managed and treated in line with the HCPC risk appetite.

11. Responsibilities

Responsibilities for the HCPC Operational Risk Management Policy are:

- The **Council** is responsible for setting the HCPC risk appetite and for ensuring that risk is being managed in line with company objectives.
- **The SMT** is responsible for reviewing and approving the ORM process, providing support for embedding the process across the organisation and providing an escalation point for critical risks.

- The **Chief Information Security & Risk Officer** is responsible for coordinating the ORM process, supporting risk owners and delivering periodic risk reporting to the SMT.
- **Risk owners** are responsible for managing their allocated risks in line with the ORM process.
- **All employees** are responsible for reporting potential risks to their departmental managers.

Individuals who have any questions or concerns about this policy should contact the policy owner.

12. Review Period

This document will be reviewed on an annual basis or following a significant business change.

13. Document Control

Doc Ref	HCPC Operational Risk Management Policy	**Publication Date**	
Owner		**Role**	
Authorised By		**Role**	

14. Document History

Issue	Reason for Change	Date
0.1	Draft document created	27 January 2021
0.2	Comments RD	19 March 2021
0.3	Updated following comments from Claire Amor	29 March 2021

Operational Risk Management Guide

1. Introduction

To maintain and improve the level of service HCPC delivers to its stakeholders, the organisation must understand and manage the risks it faces. Risks are inherent to HCPC activities and can relate to strategic threats, operational issues, compliance with laws and contracts, and reporting obligations.

Understanding risk provides a foundation to enable effective decision making across the organisation. By accurately identifying their risks, departments can then suggest treatment plans that can be input into budgeting processes to enable improvements to be adequately resourced. Assessing the impact of risk and identifying the root cause provides a strong justification for improvement proposals. Also, by implementing a consistent process across the organisation the SMT will be able to compare risks identified by different departments and allocate budget on the basis of the most effective reduction in risk exposure.

1.1 What is a risk?

Risk can be defined as “the effect of uncertainty on objectives”. It can be considered to be the potential harm that a given threat or exploitation of a vulnerability will cause to HCPC assets such as company reputation, information, processes, systems, equipment or buildings. Risk can also present opportunities and the impact of these on objectives should also be considered.

To maximise the value delivered to all its stakeholders, HCPC must understand the types of risks it faces and address them appropriately. HCPC does this by managing risk based on a combination of the probability of an event and the impact of its consequences.

Operational risks in HCPC are grouped by category:

- Public Protection
- Finance
- Reputation
- Operations
- Strategy
- Information Security

1.2 Purpose and objective of the Operational Risk Management process

The purpose of the Operational Risk Management (ORM) process is to protect and enhance HCPC’s short and long term viability by managing the uncertainties that could influence the achievement of its objectives. Implementing an effective ORM process achieves the following key objectives:

- **Oversight** - All critical risks are identified and are managed and monitored in line with the HCPC risk appetite.
- **Ownership and Responsibility** - The ownership of a risk is assigned to a named role that is responsible for risk identification, evaluation, mitigation and reporting.
- **Assurance** – The HCPC Senior Management Team (SMT) has assurance that risks are being appropriately and consistently managed.

1.3 The HCPC Approach to ORM

ORM is a framework applied by HCPC management and staff to identify potential events that may affect HCPC, manage the associated risks (and opportunities) and provide assurance that HCPC objectives will be achieved.

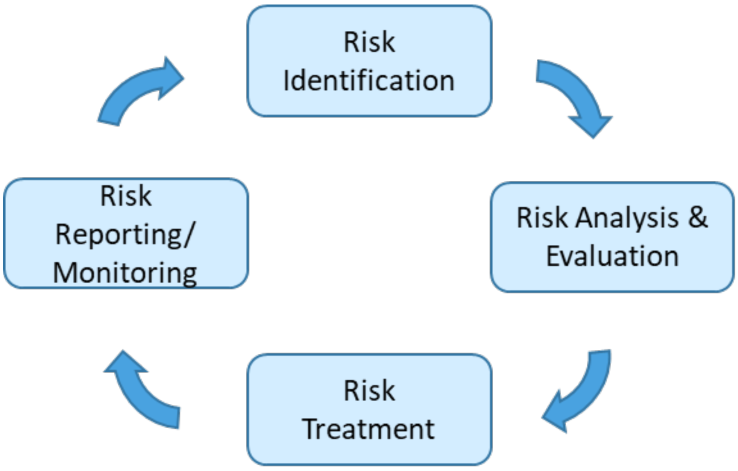
Through this approach to risk management, HCPC can:

- Ensure prompt resolution of internally identified risks to ensure compliance with laws, regulations and contracts.
- Deliver a more efficient use of capital and resources.
- Reduce the likelihood of operational errors.
- Be subject to lower compliance/auditing costs.
- Be subject to fewer surprises.

- Focus on lower cost prevention rather than higher cost resolution strategies.
- Benefit from an increased awareness and consistent view of risks (existing and emerging).
- Deploy a consistent, repeatable approach to mitigate risks and identify opportunities.

2. The ORM Process

The ORM process within HCPC is an on-going and cyclical process with four primary steps:



The effective implementation of these steps requires:

- The SMT to set the tone for risk management across the company.
- The Council to define the risk appetite.
- The SMT to define how risks will be identified, evaluated and managed.
- All staff to contribute to the identification, evaluation and treatment of risks.

It is important to ensure that risks are re-evaluated and updated on an on-going basis to reflect new information and experiences so that all significant risks and opportunities are appropriately identified and addressed.
ORM requires involvement from all HCPC departments and requires management to understand the risks facing their departments, create appropriate treatment plans for the risks identified and maintain these risks within the risk appetite set by the SMT.

2.1 Risk Appetite and Tolerance

Risk appetite is the level of risk the organisation is prepared to accept. Within HCPC it will be agreed by the SMT for each of the 7 risk categories detailed above.

Specific risks may straddle more than 1 risk category and in such cases the risk category with the lowest risk appetite will be used to determine the risk response and associated treatment.

The HCPC risk appetite is detailed in the following document:

- Risk Appetite Statement February 2021

A summary of the risk appetite is listed in Appendix A.

2.2 Process Methodology

The ORM process ensures that there are common definitions, language, categorisations, and methodology used when managing risk.

There will be a single Operational Risk Register (Operational Register) containing risks from across all HCPC departments. These risks will typically be owned by either the senior department manager or a nominated subject matter expert from within these departments. This Operational Register will be monitored by the Chief Information Security & Risk Officer and will be periodically reviewed by the SMT.

3. The Process Steps

3.1 Risk Identification

The purpose of risk identification is to identify sources of risk and define their related risk event, cause and consequences. This step should also identify an appropriate Risk Owner.

Risk identification is about understanding what might happen and who is accountable. It ensures that a comprehensive list of risks is gathered that is based on events which may occur and which may have an impact on the achievement of company objectives (in terms of enhancing, preventing, degrading or delaying the achievement of objectives).

The risk identification process should try to answer these questions:

- What could occur?
- What could it impact?
- Where could it occur?
- Why could it occur?
- How could it occur?

Risk identification should be an output from a range of business activities that can include:

- Incident analysis
- Problem management
- Internal audits
- External audits and reviews
- Process monitoring
- Process reviews
- Project lesson learnt meetings.
- Risk workshops
- Industry trends/issues

In addition to these sources, the Chief Information Security & Risk Officer may undertake formal risk assessments (see section 4) in line with SMT requirements.

Once a potential risk has been identified it needs to be defined. The key to this is detailing the cause that leads to a risk and the resulting consequences. Care should be taken when defining a risk to:

- Not state a missing or failed control (for example, a lack of system access controls), rather than the actual risk event (for example, breach of confidentiality).
- Not state an already existing issue rather than an event which has the potential to occur.

A well-defined risk statement will consist of three elements:

- Event - The occurrence that will potentially affect the company.
- Cause - Factors that trigger or lead to a risk event occurring.
- Consequence - The impact on the Company if the event occurs.

For example:

- Event - Unapproved individuals gaining access to sensitive systems.
- Consequence – A breach of information confidentiality.

- Cause – A lack of system access controls.

Meaning the risk statement would be:

- Unapproved individuals gaining access to sensitive systems may lead to a breach of information confidentiality due to a lack of system access controls.

A Risk Owner should also be allocated. This is the person with the accountability and authority to manage the risk and is usually directly responsible for the strategy, activity or function that relates to the risk. Typically, this means they will either be the senior department manager or a nominated subject matter expert from within the department. In the latter case, this could happen when an individual is responsible for the day-to-day management of a key asset and therefore is more directly responsible for it than the Asset Owner whose responsibility is more centred on oversight.

3.2 Risk Analysis and Evaluation

The purpose of this step is to develop a more detailed understanding of the risk in order to understand its importance and ensure it is handled consistently.

Risk analysis and evaluation involves:

- Considering current controls and their effectiveness
- Analysing the likelihood of the risk occurring
- Analysing the consequences of the risk
- Determining the current risk rating.

The risk rating is determined by considering:

- The likelihood of the risk occurring.
- The impact on HCPC if the risk occurs.

The likelihood of the risk occurring is often based on the probability or number of times the risk might occur over a specified time frame such as daily, quarterly, yearly etc. A higher probability or frequency of the event occurring will result in a higher likelihood score. An event that is expected to occur sooner rather than later will also result in a higher likelihood.

The impact of the risk occurring can sometimes be quantified (e.g., monetary impact) but can also be described in qualitative terms (e.g., reputational, service quality or regulatory compliance impact). The magnitude or severity of a risk is based on the product of its likelihood and impact.

The type of information used to support risk analysis and evaluation can include:

- Company history and experience
- Industry information and experience (both local and international)
- Relevant incident data
- Market insights and competitor analysis
- Subject matter expertise and insights

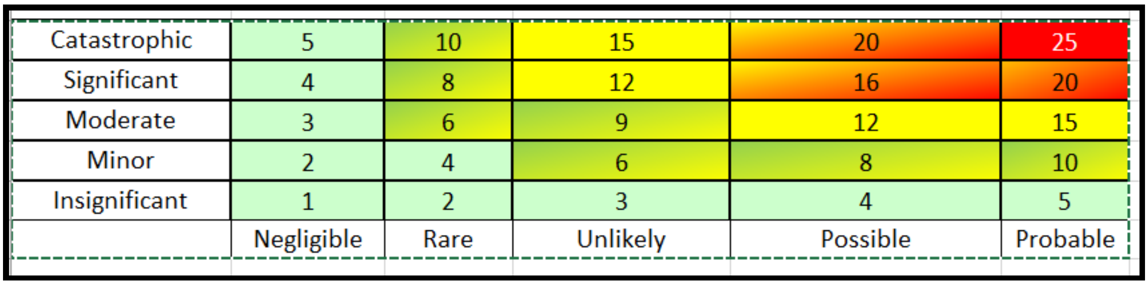
While analysing and evaluating a risk, the Risk Owner should identify the current controls and treatment plans in place and examine their effectiveness in reducing the likelihood and impact of the risk.

To support the risk analysis and evaluation and ensure that it is undertaken in a consistent manner across all departments and for all risks, there are standard HCPC risk likelihood and risk consequence tables for the risk to be assessed against.

The risk likelihood table and the risk consequence table are detailed in Appendices B and C.

The risk consequence table provides consequence ratings against each of the 6 risk categories. Risks will often fall into more than one category, where this is the case the highest impact across the relevant categories should be used for the risk.

Once risk analysis and evaluation has been completed, risks can then be plotted on a risk map, as shown below:



Catastrophic	5	10	15	20	25
Significant	4	8	12	16	20
Moderate	3	6	9	12	15
Minor	2	4	6	8	10
Insignificant	1	2	3	4	5
	Negligible	Rare	Unlikely	Possible	Probable

Levels of risk are defined as;

- Low, 1 – 5 (pale green)
- Low / Medium, 6 – 10 (yellow green)
- Medium, 11 – 15 (yellow)
- Medium / High, 16 – 20 (yellow red)
- High, 21 – 25 (red)

3.3 Risk Treatment

The purpose of the risk treatment step is to decide whether or not the current risk rating is acceptable or requires additional action (referred to as risk treatment). The response to a risk generally falls into one of four categories:

Response	Definition
Accept	Accept, manage and monitor the risk. No action to reduce.
Mitigate	Accept some of the risk. Introduce controls/mitigation to reduce the risk to within accepted risk appetite and tolerance
Transfer	Transfer the risk to a third party. e.g., obtain insurance or outsource the activity to another company
Avoid	The risk is too great even after potential mitigation and therefore the activity associated with the risk should be stopped

The response will depend upon the agreed risk appetite for the risk category.

If the risk is above the agreed risk appetite then a treatment plan will need to be formed that either mitigates, transfers or avoids the risk. Mitigation actions are measures that will manage the risk by reducing its likelihood and/or its impact.

Typically, the Risk Owner will need to work closely with a variety of subject matter experts to identify the most effective and appropriate mitigation actions and agree who should be responsible for implementing them.

When determining mitigation actions, it is important that the target risk rating is agreed (i.e., the level of risk that will remain once the treatment plan is complete). Cost versus business benefit will often mean that it is not possible to completely eradicate a risk and the aim of the mitigation actions in this situation are to bring the risk exposure level down below the agreed risk appetite for the risk category.

3.4 Risk Reporting and Monitoring

The purpose of the risk reporting and monitoring step is to ensure risks and treatment activities are reviewed on a regular basis to ensure that risks remain within acceptable levels and treatment activities achieve their objectives in agreed timescales.

HCPC priorities and the areas it operates in change over time and this means that the likelihood and impact of already identified risks may also change over time. Therefore, ORM needs to be an ongoing process in which risks, controls and risk response activities are continuously monitored, reviewed and updated to reflect progress and changing circumstances.

Risk Owners should review their risks and associated treatment plans on a regular basis to ensure that their risk information is kept current. The frequency of these reviews should be agreed with the Chief Information Security & Risk Officer and will be dependent on the level of risk and the timescales of treatment plans being implemented. As a default it would be expected that all risks would be reviewed at least quarterly. However, risks that have a rating of Low or have been accepted or have a long term treatment plan may be reviewed less frequently. Risks with a rating of High would typically be expected to be reviewed more frequently.

The SMT requires the results of the ORM process to be periodically reported to them in their oversight capacity and to gain assurance that risks are being proactively managed in line with the agreed risk appetite. The Chief Information Security & Risk Officer playing an oversight role to ensure that risks are being appropriately managed and monitored.

4. Risk Assessment

Where required the Chief Information Security & Risk Officer will undertake formal risk assessments. The aim of a risk assessment is to complete the risk identification and risk analysis and evaluation stages of the risk management lifecycle for a specified scope and in response to a specific requirement of the organisation. Risk assessments can be initiated due to:

- Significant change within the business.
- New or changed key services.
- New or changed supplier relationships.
- New or changed customer or other interested parties' requirements.
- New or changed resources (e.g., data centres, offices etc.) or technologies.
- Any other significant improvement projects or opportunities.
- Significant events and incidents.
- Significant business continuity events and exercises.

The scope of a risk assessment can vary depending on the requirements of the business. It is therefore important that the scope is clearly defined and documented at the start of the process. This scope should document the objectives of the risk assessment, its boundaries (e.g., a specific supplier, team, process etc.) and the risk assessment methodology used.

Once the scope is defined, a risk assessment should consist of the following steps:

- Asset identification
- Threat identification
- Existing control identification
- Vulnerability identification
- Risk identification
- Risk evaluation.

4.1 Asset Identification

An asset is anything that has value to the organisation, it can be tangible (e.g., software, documentation) or intangible (e.g., brand, staff morale).

Asset identification should be performed at a level of detail to provide sufficient information for the risk assessment. This level of detail will influence the overall amount of information collected during the risk assessment and the granularity of risks identified. For example, if a risk assessment is being carried out at an organisation level, end user computing assets can probably be identified at a high level such as laptops, desktops, mobile phones etc. However, if the Technology department is carrying out a risk assessment on computer hardware, it is likely that end user computing assets will need to be broken down into a greater level of detail, for example each type of laptop issued to users. This will ensure that the risk assessment is identifying the right level of risk. If required, the level of asset identification can be refined in further iterations of the risk assessment process.

Once identified, each asset needs to have a value associated with it. For risk assessments being driven by information security requirements, the following asset valuation matrix should be used:

Value	Value Name	Value Description
1	Insignificant	Insignificant
2	Moderate	Moderate impact which can be effectively managed
3	Significant	Significant impact which requires active involvement from senior staff to contain
4	Major	Major impact, immediate action required to prevent affecting long term prospects for company
5	Catastrophic	Potentially catastrophic impact upon long term business due to non-renewal of contracts and reputational damage within industry

If required (for example, because the risk assessment is being driven by other criteria such as financial requirements) other valuation criteria such as replacement costs can be added. However, for consistency the valuation levels should be kept consistent. The asset owner will often be a good source of information concerning asset valuations.

4.2 Threat Identification

A threat has the potential to harm assets, it can be of human origin (e.g., user error, hacking) or of natural origin (e.g., flood, fire). Threat sources can be accidental (e.g., user error) or deliberate (e.g., hacking) and can arise from within or from outside the organization.

During the risk assessment, threats should be identified generically and by type (e.g., physical damage, technical failure) and then, where appropriate individual threats within the generic class should be identified. Threats may affect more than one asset, and, in such cases, it is likely that they will have differing impacts on each asset.

4.3 Existing Control Identification

It is important to identify existing controls to ensure unnecessary work or cost is avoided. When identifying controls, care should be taken to document which assets they are relevant to and their level of maturity.

4.4 Vulnerability Identification

A vulnerability is a known weakness or issue related to an asset which can potentially be exploited by a threat. Vulnerabilities can be identified in the following areas:

- Organisation
- Processes and procedures
- Management routines
- Personnel
- Physical environment
- Information system configuration
- Technology equipment
- Third party dependence

Asset owners and teams/individuals who frequently work with the assets are likely to be good sources of vulnerability information.

4.5 Risk Identification

Risks can be identified by reviewing:

- The identified asset values.
- The likelihood and impact of threats associated with these assets.
- The asset vulnerabilities that can be exploited by these threats.
- The maturity of the controls protecting these assets from these threats.

When identifying risks during a risk assessment the guidance detailed in the risk identification section above should be followed.

4.6 Risk Analysis and Evaluation

The risk analysis and evaluation step of a risk assessment should follow the guidance details in the risk analysis and evaluation section above.

5. Supplier Risk Assessment

Suppliers that are deemed to be an extreme or high information security risk because, for example, they are delivering business critical services, require access to the HCPC network or require access to confidential information will be subjected to a supplier risk assessment. Dependant on the business requirements, supplier risk assessments can be undertaken before suppliers are formally engaged, after significant changes to their services or organisation and (if deemed necessary) on a periodic basis. Supplier risk assessments follow the same steps as other types of risk assessment with the following additional guidance:

- Asset identification - All assets the supplier will have access to, should be identified.
- Threat identification - The threats the supplier presents to the identified assets should be identified.
- Existing control identification - The HCPC and supplier controls that will mitigate identified threats should be identified.
- Vulnerability identification - Any vulnerabilities associated with the identified assets or supplier vulnerabilities relevant to the services or systems they are supplying should be identified.
- Risk identification - Based on the previous 4 steps, potential risks should be identified.
- Risk analysis and evaluation - The potential risks should be evaluated to determine whether they should be managed as HCPC risks or should be passed to the supplier to mitigate as a requirement of their contract.

6. Roles and Responsibilities

The following table summarises the roles and responsibilities with respect to the ORM process:

Senior Management Team (SMT)	• Review and approve the ORM process. • Provide support for embedding the ORM process across the Company. • Set the ORM risk appetite level. • Provide ORM oversight. • Ensure key strategic risks are managed in line with HCPC objectives. • Act as an escalation point for critical risks.
Chief Information Security & Risk Officer	• Manage the ORM process. • Undertake risk assessments. • Embed the ORM process across HCPC.

	- Support Risk Owners in executing the ORM steps. - Provide the SMT with regular ORM reporting.
Risk Owners	- Manage allocated risks ensuring they are correctly identified, assessed and measured in line with the ORM process. - Ensure appropriate risk responses are agreed and actioned in line with the ORM process. - Monitor allocated risks ensuring risk responses are tracked and risks are periodically reviewed. - Provide the Chief Information Security & Risk Officer with regular risk status updates.
Treatment Owners	- Manage allocated risk response actions. - Provide the Risk Owner with regular risk response status updates

7. Review Period

This document will be reviewed on an annual basis or following a significant business change.

8. Document Control

Doc Ref	HCPC Operational Risk Management Process	**Publication Date**	
Owner		**Role**	
Authorized By		**Role**	

9. Document History

Issue	Reason for Change	Date
0.1	Draft document produced	27 January 2021
0.2	Updated following comments from Roy Dunn	23 March 2021
0.3	Updated following comments from Claire Amor	29 March 2021
1.0	Updated with new split of risk Scale, L,L/M, M, M/H,H	9 Sept 2021

Appendix A – Risk Appetite

The HCPC risk appetite statement as documented by the Council on 25 February 20201 is:

Risk Appetite Statement

Our vision is to be a high performing, adaptable and caring regulator that ensures public protection through strong, evidence-based regulation. The HCPC has agreed the following statement of its appetite for taking risk in the furtherance of achieving this vision.

Regulatory Quality - Open

How will we deliver effective regulatory functions?

- Our focus is on long term and lasting quality in our regulatory delivery. We have to take risk and challenge ourselves to achieve positive change. Sticking with a low risk status quo will limit our progress.
- We are open to risks that will further us in our aim of delivering excellent regulatory functions.
- We are prepared to try new approaches that do not have a guarantee of success where the potential benefits of success outweigh the consequences of failure.
- We proactively seek to reduce public protection risk through the promotion of professionalism and prevention.
- The risks we are willing to take do not have a significant chance of long-term negative impacts on our regulatory quality. We accept that in striving for excellence and trying new approaches, short term issues may arise which we will seek to mitigate as best we can.
- It is essential that mitigations to ensure ongoing public protection are in place as a foundation of taking risks to improve our regulatory quality.

Compliance – Measured

How will we comply with our statutory, regulatory and policy requirements?

- We have a preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.
- We are willing to take decisions that could be challenged only where we are confident, we would be successful in defending against such challenge, and the adverse consequences of being unsuccessful are minimal.
- We are willing to take low level risks of negative PSA performance impact given the appropriate controls are in place and we consider the potential benefits are required to maintain or improve our PSA standard performance.
- It is essential that the long-term achievement of PSA standards is assured.

Communication and Profile – Seeks

How will we be viewed by our stakeholders?

- We are eager to be innovative in content and method in order to communicate more effectively, despite greater inherent risk.
- We are willing to express our views and communicate on issues where stakeholder opinion is divided, but where the HCPC has a legitimate voice and the Council has an agreed policy position.

- In communicating our views, we are willing to accept the possibility of manageable reputational risk or a negative, but not irreversible, impact on a stakeholder relationship.
- We acknowledge that being bold in communicating our position may lead to increased scrutiny from stakeholders. We accept this risk as being necessary to enable the HCPC to assert its voice and shape debate in the furtherance of excellence in regulation.
- We seek meaningful two way dialogue with our stakeholders, even where this may pose a risk to our profile due to uncomfortable feedback.
- It is essential that the HCPC's voice is not perceived to be party political. The HCPC is neutral as a public body.

People – Seeks
How will we lead our workforce?

- We are eager to be innovative and to choose options that increase our effectiveness as an organisation despite greater inherent risk.
- We are prepared to accept risk as long as there is the potential for improving culture, recruitment and retention.
- We want to innovate to improve our culture and working environment.
- We are willing to review and restructure where this is needed, accepting the potential for short term disruption in order for the HCPC to benefit from better ways of working.
- It is essential that risk taking in this area is consistent with the HCPC's values and culture. As an employer are committed to upholding and promoting Equality, Diversity and Inclusion.

Financial and Value for Money – Measured
How will we use our resources?

- We are prepared to accept possibility of limit ed financial loss where it does not have the potential to impact on our going concern.
- Value for money is our primary concern in financial expenditure but we are willing to consider other benefits or constraints.
- We are funded through registrant fees and we have a responsibility to ensure we invest cautiously to minimise loss while maximising benefit.
- We accept that investments may be long term and take time to deliver rewards, appropriate benefit realisation monitoring is required to mitigate risk in investments.
- It is essential we remain a financially viable organisation to ensure continued public protection through continued operation. Significant financial risks are not compatible with this requirement.

Appendix B – Risk Likelihood Table

	Strategic	Programme/Project	Operational
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**	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**	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**	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.

Appendix C – Risk Impact Table

	Public Protection	Finance	Reputation	Operations	Strategy	Information Security
Catastrophic	A systematic failure for which HCPC is ultimately responsible. 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.	Services to stakeholders are unavailable for an extended period of time (days)	Strategy rendered invalid	Significant breach of confidential information involving extensive quantities of data. Regulatory investigation required
Significant	A systematic failure for which HCPC is ultimately responsible. 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.	Services to stakeholders are unavailable for a significant period of time (hours)	Progress on multiple strategic objectives is stopped.	Significant breach of confidential information involving limited quantities of data. Regulatory investigation required.
Moderate	A systemic failure for which HCPC is ultimately responsible. 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.	Services to stakeholders are significantly disrupted. Services are degraded or responses are slow for an extended period of time (days).	Progress on 1 strategic objective is stopped.	Limited breach of confidential information No regulatory investigation required
Minor	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.	Services to stakeholders are disrupted. Services are degraded or responses are slow for a significant period of time (hours)	Progress on multiple strategic objectives is slowed.	Significant or widespread non-compliance to information security policy by staff. No breach of confidential information
Insignificant	A systemic failure which fails to address an operational requirement	Unfunded pressures under £20,000.	Event that will lead to public criticism by external stakeholders as anticipated.	Services to stakeholders are disrupted for a short period of time (minutes).	Progress on 1 strategic objective is slowed.	Minor or one-off non-compliance to information security policy by staff. No breach of confidential information

Low

Low / Medium

Medium

Medium / High

High

Operational Risk Management
Risk Owner Overview

If you are a risk owner these are the steps you need to follow:

Risk Identification

Ensure you are the right person to be owning the risk

- Are you able to accurately assess the risk's impact?
- Are you able to define a treatment for the risk?
- Are you able to effectively monitor the risk and its treatment?

Write a risk description that should be structured as: *Event – Cause – Consequence*

Ensure the risk is added to the Operational Risk Register

Risk Analysis & Evaluation

Use the HCPC risk consequence and risk likelihood tables to help you determine the risk's current likelihood and impact. When doing this take into account:

- The effectiveness of current processes and controls
- Whether incidents or issues have occurred relevant to the risk
- Advice from colleagues with subject matter expertise

When determining the risk likelihood and impact it is often useful to think about the most likely outcome rather than just the 'worse case' scenario

Risk Treatment

Determine how you are going to treat the risk. The 2 usual options are:

- **Mitigate** – Implement actions that will reduce the risk's impact and/or its likelihood to levels that are suitable for the business
- **Accept** – Monitor the risk but do not implement any actions to affect its impact or likelihood. This is often a good option if the risk currently has a low impact and/or likelihood but there is a possibility this may change over time

You could also **Avoid** the risk by stopping the activities associated with the risk or **Transfer** the risk by handing the activities to a third party When determining how you are going to treat the risk make sure your decision is in line with the **HCPC Risk Appetite Statement**

Risk Reporting/ Monitoring

Based on its impact, likelihood and treatment plan, determine how frequently you should review the risk. When reviewing the risk, you should:

- Check that the risk description, impact and likelihood are still correct, taking into account any changes in HCPC and any effects treatment actions have had
- Review the status of any treatment actions and ensure that these are still appropriate and are being progressed effectively
- Ensure all the risk details in the Operational Risk Register are up to date