Audit and Risk Assurance Committee

16 September 2021

health & care professions council

Internal Audit report – Risk Management

Executive Summary

As part of the 2021-22 Internal Audit Plan as approved by the Committee, BDO LLP have undertaken a review of the HCPC's Risk Management.

The objective of the audit was to provide assurance that the new process, policy and principles are properly designed so that they can embed effectively, particularly the operational risk management process and its link to organisational strategy.

Previous consideration	None.
Decision	The Committee is invited to discuss the report.
Next steps	Recommended actions agreed with the Executive will be tracked for progress in the Committee's standing recommendation tracker report.
Strategic priority	All
Risk	• The risk framework design and approach is suitable and sound. • Good progress is being made regarding operational risks being identified, assessed and properly escalated to senior management. • Risks, including operational risks, are linked coherently to HCPC's strategy. • Specific risks, as case studies, are being managed as stated in the risk register.
Financial and resource implications	The cost of the audit is included in the Internal Audit annual fee.
Author	BDO LLP

HEALTH & CARE PROFESSIONS COUNCIL

INTERNAL AUDIT REPORT - FINAL

RISK MANAGEMENT
SEPTEMBER 2021

Contents

Document history			Distribution	
FINAL	[0296398]	03/09/2021	Health & Care Professions Council	[current version]

Auditor:	Heather Buckingham
Reviewed by:	Bill Mitchell

1 Executive Summary

Introduction

1.1 This audit was completed in accordance with the approved annual Internal Audit plan for 2021/22.

1.2 Risk management is a key business management tool and HCPC have been reviewing and updating their approach to it. A new policy and process guide has been developed, a new risk appetite framework and appetite formulated, and both strategic and operational risk registers reformatted and updated. The risks have been mapped to HCPC's strategy, with operational risks reduced to some 80 risks in total. Ownership of risks has been agreed and allocated.

1.3 The reporting and updating of risks has also being modified. The Audit & Risk Assurance Committee will receive operational risks in September 2021 to provide a broader awareness of those risks to the governance body responsible for oversight of the risk management framework, on top of their planned usual review of the strategic risks and risk appetite statement. This will provide an opportunity for the Committee to define its future operational risk oversight needs. Senior management will review strategic monthly and operational risks quarterly.

1.4 There are two new members of the Senior Management Team who have joined over the last few months. This presents an opportunity for developing a fresh look at the risks and the process of risk management. Another risk is that operational risks are not satisfactorily escalated or they are not sufficiently linked to the organisational strategy, particularly given that many more are involved with the registers' content.

Review objectives and approach

1.5 The objective of the audit was to provide assurance that the new process, policy and principles are properly designed so that they can embed effectively, particularly the operational risk management process and its link to organisational strategy. The key risks with this area of activity were whether:

- The risk framework design and approach is suitable and sound.
- Good progress is being made regarding operational risks being identified, assessed and properly escalated to senior management.
- Risks, including operational risks, are linked coherently to HCPC's strategy.
- Specific risks, as case studies, are being managed as stated in the risk register.

1.1 Our approach was to conduct interviews to establish the processes that have been designed relating to risk management. We then obtained and reviewed relevant documentation to evaluate the design of the processes and confirmed that they have been built as described. We then undertook sample testing as required for three risk areas in order to confirm that controls were operating as intended.

Key conclusions

🟩🟧 (Green-Amber)	Generally a good control framework is in place. However, some minor weaknesses have been identified in the control framework or areas of non-compliance which may put achievement of system or business objectives at risk.

1.2 HCPC have developed a robust operational and strategic risk management framework which encompasses a more mature approach, including monthly reviews by ELT of the strategic risks and planned quarterly reviews of operational risks.

1.3 The new approach to risk management overall has received good buy-in from management and Council, notably being more strategically focused with a welcome discussion on risk appetite. Council see risk management now as being given the right priority and a means for open discussion with management. This demonstrates HCPC's commitment to risk management across the organisation and 'setting the right tone from the top'. Policies and guidance are up to date and reflect the current operational risk management methodology. The 'one page guide' allows staff efficient and effective information on operational risk management procedures and policy in one document.

1.4 As planned, risk workshops with each department in HCPC have been undertaken successfully to ascertain operational risks, which were hosted by an external risk facilitator. The outputs were then reconciled to strategic risks to ensure an appropriate read across between the two and identify any potential gaps. The two-fold process enabled both a 'bottom up' view of operational risks, and a means by which strategic risks be linked to them. The operational risk register is sufficiently comprehensive, yet not overwhelming in size to manage going forward.

1.5 We sampled several risks in detail, to ascertain whether the risk assessment process followed and the mitigations asserted on the register are in place (and any further mitigations being pursued). We examined risks relating to facilities management, GDPR and partners. We found that all risks tested were recorded in the risk register consistently, with appropriate risk owners in place, and with mitigations in evidence. This further demonstrated the adoption and buy-in to the new methodology. The risks evaluated are in Appendix B.

1.6 However, like any business change, the revamping of an operational risk management process takes time to bed-in fully. We examined only one cycle of the operational risk management (risk identification to review process), as the process is very new. Future review cycles, planned to be quarterly, will need to ensure that they retain good levels of engagement within departments. We are confident that providing continued support from the corporate centre, the operational risk review process is sustainable and will continue to add value.

1.7 Notwithstanding the overall positive findings, the operational risk management process, guide and policy does not directly cover the consideration of risks for key business decision making events such as: business cases, business planning and project management. We consider that it is key that the risk methodology should be applied in a similar way in these key instances of business activity. Otherwise, the operational and strategic risk activities are disconnected with or inconsistently applied to key routine business activities.

1.8 We also consider that an ARAC deep dive into operational risks, on a cyclical basis, would enhance the visibility of operational risks to the committee and strengthen the governance of HCPC. ELT members would be invited to discuss the strategic and operational risks relating to their responsibilities at ARAC.

1.9 In addition, we had some minor suggestions for management's consideration regarding the guidance documents. These are referenced in the Appendix A.

Recommendations summary table

1.10 The following table summarises the recommendations made across the key risks audited, grouped by priority ratings:

	Key risk area	Rating		Recommendation Priority rating		
				1	2	3
1	Risk framework design	Green	Amber	-	2	-
2	Identification and risk assessment	Green		-	-	-
3	Operational risks and the strategy	Green		-	-	-
4	Risk register accuracy	Green	Amber	-	-	-
	Total recommendations made			**-**	**2**	**-**

1.11 The following tables in Section 2 Key Findings show the results of our analysis by each key risk area. Areas for improvement are highlighted with the key recommendations in the right-hand columns.

2 Key Findings

Key Risk Area 1: Risk framework design

Assessment: Green Amber

Background

Risk management frameworks for any organisation should include five crucial components, these are: risk identification, risk measurement & assessment, risk mitigation, risk reporting & monitoring and risk governance. We reviewed the strategic and operational risk frameworks in place to verify if all five components are in place and working effectively across the organisation.

1.1 Policies and guidance

Findings & implication	Recommendation
Positive findings - A clear and comprehensive project was developed to uplift the strategic and operational risk management process including the risk management guides, one-page guide and policy documents. A longer policy document exists as well as a full guide. These documents cover the key steps normally expected, in a clear way. - The full guide to operational risks gives reference to risk assessments in procurement, thus looks beyond the process of completing and reviewing risk registers and the activity that generates and reflects. - The summary one-page is a handy guide to remind staff of the operational risk management process, avoiding the need for them to navigate the full guide. **Areas for improvement and implication** - There is an operational risk policy and a separate strategic risk policy. While it is helpful to direct staff to the relevant guidance for them to avoid confusion, they are part of the same risk framework and there is a small risk of confusion, therefore, where there are a number of documents in play relaying similar information. - The summary operational risks policy document – the guide to risk owners – makes little reference to how to think and apply risk management in situations where managers are deciding upon	1. We recommend the one-page and full policy documentation should be: - Either encompass one document containing strategic and operational risk management policies and procedures, or at least signpost to each other's policy and guidance documentation; - reference how to think about the risks and conduct risk management in areas where managers are deciding upon suppliers and partners, business cases, business planning and projects should be referenced in the full and signposted in the one-pager guide; - require project risks to use the same assessment method and format. ***Priority 2*** **Management response**

Findings & implication	Recommendation
suppliers and partners, business cases and business planning, and projects. Other guides relating to those policies may give more detail regarding risk considerations, but where these are not signposted within the one-pager guide not specific references made. Incorporation of these aspects of managing risk in the guidance will help to integrate risk management processes in • Project risks currently use the previous methodology for risk management and thus there is a disconnect between project risks and those risk assessments undertaken against the rest of the organisation. • *Further minor observations of how the full guide can be strengthened can be found in Appendix A of this report.*	**Accept** **Action:** New projects commencing from now will use a new risk framework based on the new operational risk register, however, PM activities require an enhanced level of detail which will be additional to the regular operational risk register format. Existing projects will not be updated to the new format **CISRO to** • liaise with Head of Projects to implement the new approach to risk registers for the project risk registers. • Update the risk management policy to be an all-in-one document covering strategic risk as well as operational risk and a section on risk in selecting suppliers and business cases. The HCPC has recently developed a new business case template and consideration of risk will be made more explicit. **Action Owner:** CISRO **Completion date:** by end of 2021

1.2 Consistent risk management integration across the business

Findings & implication

Positive findings

- Heads of department have been coached by an external consultant, to help them understand the risk process and develop a fresh set of operational risks, including ensuring existing and new heads would be operating at the same level of understanding.
- The update of the HCPC risk appetite and its integration into the thinking behind the development of strategic and operational risks, has advanced the maturity of the risk framework.
- A review mechanism for risks has been set up – monthly at ELT for the strategic risks and quarterly for the operational risks. We consider this frequency to be sound, as it sits well with the upward reporting processes.
- Council members consider risk management to now be well thought through, focussed much more on strategic priorities and welcomed the risk appetite discussions as being the biggest gap in the recent past but now addressed satisfactorily. Council noted that they are much more confident about management's approach to, and openness about, risk.

Areas for improvement and implication

- ARAC do not undertake reviews of operational risks as a matter of routine. To do this across all risks for each ARAC would be a significant undertaking and diminish ARAC's effectiveness, but deep dives on specific departments of strategic risk themes would strengthen oversight, governance and assurance on the operational risk management process itself.
- The review of operational risks is not a standing agenda item at departmental level team meetings. There is a risk where risks are not diarised and regularly considered the process does not remain 'live' and is not used as a key tool for heads' evaluation of performance and the progress in making changes.

Recommendation

2. ARAC should conduct deep dives on operational risks grouped by the strategy area or strategic risk on a cycle. This would give Council comfort that the operational risk management process and the management of risks. The responsible director would attend the relevant deep dive, with a role for the Quality Assurance team providing assurance around mitigations.

Priority 2

Management response

2. Accept

Action: Accepted in principle though it is for ARAC to agree they wish to take this approach. Operational risk will be presented to ARAC in September to frame discussion on ARACs ongoing engagement with operational risk for agreement

Action Owner: Head of Governance

Completion date: Discussion to be held in September. Next meeting in November would determine if action is closed or not.

Key Risk Area 2: Identification and risk assessment

Assessment: Green

Background

To have an effective strategic risk register which encompasses the key risks to the organisation it is imperative to have both a top down and a bottom-up approach to risk identification, assessment and escalation. We interviewed key staff to verify the process for the identification, assessment and escalation of operational risks to senior management to verify if the process in place is robust and sound.

Findings & implication

Positive findings

- Council members consider the overview on risk is the priority for them, which the new process fulfils. It was too early for them to comment on operational risk reporting from a Council perspective, but feedback suggests they are content with the process to date.
- Our interviews concluded that management, including the CEO, are happy with the process of formulating the new risk registers, the new framework and the quality and completeness of the operational risk registers and were engaged with developing it.
- A clear range of operational risks have been developed, with external assistance to develop the first iteration following an intense, externally facilitated series of workshops.
- The risks identified by each team are much more succinct than previously – for example: fewer risks, better crafted wording and all on one spreadsheet. This has the double benefit of enforcing a better prioritisation of effort and reduces the sense of the review process being an unnecessary or arduous burden.

Recommendation

None

✓

Management response

N/A

Key Risk Area 3: Operational risks and the strategy

Assessment: Green

Background

It is important for all key operational risks to be identified and then assessed at how they can affect the organisations strategy and affect the ability for organisations to achieve both their operational and strategic objectives. We interviewed key staff and reviewed the content and output of the risk workshop to verify how operational risks, strategic risks and the strategy were observed and covered by senior management.

Findings & implication

Positive findings

- Workshops did not focus on the organisation’s strategic objectives. This was a deliberate decision, which we endorse: workshop activity could have easily gotten drawn into a reinvention of strategic risks and not drawn out the operational risks – the primary purpose of the exercise.
- Strategic risks and strategy have been reconciled to the outputs from the operational risk workshops by the ‘core risk team’, which has helped to ensure an appropriate read across between the two, to identify any omissions in the operational or strategic risk registers.

Recommendation

None

✓

Management response

N/A

Key Risk Area 4 : Risk register accuracy

Assessment: Green Amber

Background

Having an up to date risk register in place that demonstrates the true position of the risks for an organisation is imperative to ensuring effective risk management across the organisation. We tested three business areas or activities (Data Protection, Facilities and Partners) across the organisation and assessed whether the risks within each area were a true reflection of the current risk status. We interviewed staff on their experiences of the recent operational risk relaunch.

Findings & implication

Positive findings

- We found that risk owners are aware of their responsibilities and are clear that risks need to be monitored on a regular basis. They demonstrated good knowledge of the risks associated with area and are confident to translate information throughout HCPC.
- Risks are currently scored taking account of current mitigations (impact and likelihood) and scored in line with set parameters. We found this approach was applied consistently across all three areas sampled.
- Officers are clear how risks are to be escalated and who they should speak to if they have any concerns.
- We found good evidence of treatment in action and explanations were in place for Data Protection, Facilities and Partners' risk registers.

See Appendix B for further detail of risks assessed and our findings.

Areas for improvement & implication

- There were minor findings from our review of the risks, which are noted in the Appendix.

Recommendation

None

✓

Management response

N/A

A Observations to be considered

Observation KRA references	
Full Guide (KRA 1)	• The full guide should state more clearly and upfront that the role of the CISRO – facilitator of risks and not the owner. It says what his role is but needs to say what his role is not. The point cannot be emphasised enough. • The full guide refers to specific risk categories. We consider the risk categories need to be broader – they exclude risk categories such as legal, fraud, data, health and safety, etc. • Greater clarity is required on whether the risk scores are relating to inherent or residual risk (since the concept of inherent and residual risk is not made and there is no requirement to separate them)
Risk Workshops (KRA 3)	• While the focus of the operational risk workshops was on operational risks and thus not distracted by the strategic risks and the HCPC strategy, we consider it would be a better process to dedicate the last quarter of the operational risk register review workshops in future to discuss risks that relate to the strategy. Introducing the strategy near the end of the session enables the main part of the session not to be obscured by the strategy but it will allow operational leads to reflect on the risks that they might own that have an impact on strategy.
Communications of the process (KRA 4)	• One of the three officers interviewed expressed that the risk register is formally updated every six months – this should be three months and thus better communications of deadlines should be enforced and reminded to staff. (Observation not a rec).
General comments on risk registers (KRA 4)	• Target risk rating needs to be clear where the RAG rating colour is the same as the current risk rating. • There needs to be check on whether risk mitigation recorded affect likelihood or impact and these effects correspond with the assessment scores. For example, a mitigation measure that reduces likelihood always reduces the likelihood on the risk assessment. • The risk register for partners is out of date and not reflective of current deadlines for the implementation of new mitigations. Staff shortages have been cited for the delay. Whilst the risks remain constant there is insufficient information to explain the current hold up on the delivery of treatment targets. For example, due to an ongoing tribunal. Therefore, the treatment steps will not be completed until after the tribunal and therefore it would be best practice for smaller milestones to be included within the register.

B Risks assessed

Facilities

Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihooc	Risk Rating	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating	Next Review Date	Risk Status Notes
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	Medium	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	
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	High		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	
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	High		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	

Partners

Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihooc	Risk Rating	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating	Next Review Date	Risk Status Notes
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	High	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.
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	Medium	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

GDPR

Risk Number	Risk Category	Risk Title	Risk Description	Risk Team	Risk Owner	Risk Impact	Risk Likelihood	Risk Rating	Treatment Type	Treatment Steps	Treatment Owners	Treatment Target Dates	Target Risk Rating	Next Review Date	Risk Status Notes
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	High	Mitigate	Reporting culture to see where not following requirements leads to incidents, and customer mitigations for specific areas.	CISRO / Head of Governance	Sep-21	Low	Sept/Oct 2021	
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	Medium	Mitigate	Robust contracts and minimum certification requirements, to lower likelihood of breaches.	CISRO / Procurement	Sep-21	Low	Sept/Oct 2021	
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	Medium	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	

C Audit objectives, Risks & Scope

Terms of reference	
Objectives	The objective of the audit was to provide assurance that the new process, policy and principles are properly designed so that they can embed effectively, particularly the operational risk management process and its link to organisational strategy.
Key risk areas	• The risk framework design and approach is suitable and sound. • Good progress is being made regarding operational risks being identified, assessed and properly escalated to senior management. • Risks, including operational risks, are linked coherently to HCPC's strategy. • Specific risks, as case studies, are being managed as stated in the risk register.
Scope	The focus of the review was the operational risks, but the review contained an overview of the delivery of the wider risk management framework. The framework includes, risk register formulation, monitoring, reporting and review; integration into other risk management activities parts of the HCPC (in projects/programmes, partner and supplier selection, business planning and business cases). We examined specific risks as part of this review, to give insight into the accuracy of the register entries. The following risk areas are included: • Facilities • Data Protection • Partners - training The review of these topic areas were not full audits, but the outcome of our review may inform the audit planning for future reviews or audit strategies.
Approach	The review was undertaken via MS Teams interviews with key staff and review of documentation.

D Audit definitions

Opinion/conclusion	
🟩 (Green)	Overall, there is a sound control framework in place to achieve system objectives and the controls to manage the risks audited are being consistently applied. There may be some weaknesses but these are relatively small or relate to attaining higher or best practice standards.
🟩🟧 (Green-Amber)	Generally a good control framework is in place. However, some minor weaknesses have been identified in the control framework or areas of non-compliance which may put achievement of system or business objectives at risk.
🟧 (Amber)	Weaknesses have been identified in the control framework or non-compliance which put achievement of system objectives at risk. Some remedial action will be required.
🟧🟥 (Amber-Red)	Significant weaknesses have been identified in the control framework or non-compliance with controls which put achievement of system objectives at risk. Remedial action should be taken promptly.
🟥 (Red)	Fundamental weaknesses have been identified in the control framework or non-compliance with controls leaving the systems open to error or abuse. Remedial action is required as a priority.

Any areas for improvement are highlighted with the key recommendations in the right-hand columns. The symbols summarise our conclusions and are shown in the far right column of the table:

Good or reasonable practice	✓
An issue needing improvement	⚑
A key issue needing improvement	✗

Recommendation rating	
Priority ranking 1:	There is potential for financial loss, damage to the organisation’s reputation or loss of information. This may have implications for the achievement of business objectives and the recommendation should be actioned immediately.
Priority ranking 2:	There is a need to strengthen internal control or enhance business efficiency.
Priority ranking 3:	Internal control should be strengthened, but there is little risk of material loss or recommendation is of a housekeeping nature.

E Staff consulted during review

Name	Job title
Roy Dunn	Chief Information Security & Risk Officer
Claire Amor	Head of Governance
John Barwick	CEO and Registrar
David Sterling	Council & ARAC member
James McMahon	Facilities
Uta Pollmann	Partners Rep

We would like to thank these staff for the assistance provided during the completion of this review.

FOR MORE INFORMATION:

SARAH HILLARY

Sarah.Hillary@bdo.co.uk

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO Member Firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

www.bdo.co.uk

Freedom of Information Disclaimer

In the event you are required to disclose any information contained in this report by virtue of the Freedom of Information Act 2000 (“the Act”), you must notify BDO LLP promptly prior to any disclosure. You agree to pay due regard to any representations which BDO LLP makes in connection with such disclosure and you shall apply any relevant exemptions which may exist under the Act. If, following consultation with BDO LLP, you disclose this report in whole or in part, you shall ensure that any disclaimer which BDO LLP has included, or may subsequently wish to include, is reproduced in full in any copies.