Audit Committee

5 November 2019

Internal Audit report – Fraud risk assessment

Executive Summary

As part of the 2019-20 Internal Audit Plan as approved by the Committee, BDO LLP have undertaken a review to assess the HCPC's exposure to the risk of fraud and the existing controls for managing fraud risk.

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	Strategic priority 3: Ensure the organisation is fit for the future and able to anticipate and adapt to changes in the external environment
Risk	SR 3 - Failure to be a trusted regulator and meet stakeholder expectations SR 5- Failure of leadership, governance or culture
Financial and resource implications	The cost of the audit is included in the Internal Audit annual fee.
Author	BDO LLP

HEALTH & CARE PROFESSIONS COUNCIL

FRAUD RISK ASSESSMENT - FINAL

INTERNAL AUDIT REPORT
OCTOBER 2019

Contents

Page

1 Executive Summary 3

2 Key Findings 6

A Functional Standards for combatting fraud **Error! Bookmark not defined.**

B Audit objectives, Risks & Scope 20

C Audit definitions 20

D Staff consulted during review 21

Document history			Distribution	
FINAL	00296398	25/10/2019	Health & Care Professions Council	FINAL

Auditor:	Louis Dockree
Reviewed by:	Michelle Debique/Bill Mitchell

1 Executive Summary

Introduction

1.1 This audit was completed in accordance with the approved annual Internal Audit plan for 2019/20.

1.2 Fraud is an inherent risk to all organisations and it is essential that the risk is effectively managed and a clear strategy in place. Following the 2016 Fraud Landscape Review by the National Audit Office (NAO), it was identified that the Government's approach to tackling fraud had been focussed on tax and welfare, with little focus given to other areas of risk.

1.3 The NAO concluded that the true scale of fraud within the Government was unknown and there is a large disparity in the levels of reported fraud between departments. This finding extends to most other public sector organisations.

Review objectives and approach

1.4 The objective of the review was to assess the Heath and Care Professions Council's (HCPC) exposure to the risk of fraud and the existing controls for managing fraud risk.

1.5 The key risks with this area of activity are whether:

- HCPC's strategy for managing their fraud risk is appropriately designed; and
- There are adequate controls in place for preventing, deterring and detecting fraud (specifically within the main fraud risk areas).

1.6 In order to effectively manage the risk of fraud, an organisation needs to create an anti-fraud culture. This is achieved through implementing the four pillars of good fraud risk management: (a) clear strategic approach to combatting fraud; (b) raising awareness amongst staff and stakeholders; (c) implementing controls to prevent; and (d) deter fraud and having a regime for detecting and investigating fraud. Therefore in order to provide an assessment of HCPC's approach to combatting fraud we will review four pillars and provide guidance and recommendations in relation to:

- Strategic Governance in tackling fraud;
- Culture, training and Raising Concerns;
- deterrence and prevention (e.g. effective control systems); and
- detection and investigation.

Key conclusions

🟧 (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.

1.7 Overall, HCPC has a low direct exposure to fraud (where HCPC themselves will be the victim), though, HCPC's exposure is higher in relation to reputational damage as a result of a registrant committing fraud in order to gain registration, for example using false qualifications or ID documents. It is acknowledged that this is an inherent risk to regulators and is minimised through the verification procedures for registering professionals and conducting fitness to practise investigations. For example, areas of good practice include registrant due diligence, specifically in relation to verifying identity documents, references and academic/professional qualifications. Having such robust due diligence procedures allows HCPC to identify individuals who are not suitable and potentially attempting to gain registration using false information/documents.

1.8 HCPC has a good understanding of where they are most exposed to the risk of fraud and does feature on departmental risk registers. For example, within Finance and Procurement, the 'traditional' areas where fraud risk is highest, there was a good level of awareness of the risk and thus we consider that the residual risk of fraud is low. The risk of fraud within finance internally or externally is also effectively mitigated through the expected financial controls.

1.9 There is good practice is in relation to their management of conflicts of interest, not only within departments such as in procurement but also in relation to fitness to practise hearings. The Fitness to Practise team ensure that Partners adjudicating, are not conflicted. The effective management of conflicts of interest maintains the integrity of procurements and fitness to practise hearings.

1.10 Another area of good anti-fraud / cyber security is in relation to the IT project for transferring social care records to Social Work England. There is a data exchange agreement between HCPC and Social Work England outlining the agreed process and roles and responsibilities. The IT department risk assessed the options for transferring the data, opting to transfer the data using Microsoft Azure Blob storage, where Social Work England will be the administrator as they will be the ultimate data controller. The process, as described by IT, is robust in preventing data breaches in principle.

1.11 However, there were three main key areas for improvement we noted during our review:

- **Strategic Approach:** There is a weakness in HCPC's strategic approach to managing the risk of fraud. Instead the approach to combatting fraud has been managed independently by each department with no clear oversight. The risk of fraud is not specifically included, or referenced within the strategic risk register, which is reviewed by the Audit Committee on a quarterly basis. The lack of an explicit reference may result in the risk of fraud not being specifically assessed, giving the Council false assurance that the risk is being effectively managed. It should also be noted that the Audit Committee last reviewed the entire Risk Register and Risk Treatment Plan (which does include fraud and bribery more explicitly) in November 2017. In order to adopt a more strategic approach to managing fraud risk, we have recommended that the risk of fraud is more explicitly referenced within the strategic risk register. This will ensure that the risk of fraud is more effectively monitored by the Audit Committee and demonstrate a clear tone from the top.

- **Fraud Awareness:** With regards to raising fraud awareness, HCPC does not have a fraud policy and there is no fraud awareness programme across HCPC. The risk of fraud is not covered at induction or as part of an annual refresher training. A lack of fraud awareness may result in staff not being able to detect or report instances of fraud, resulting in continued losses or public protection risks, but the lack of awareness will also fail to discourage individuals from committing fraud. We have recommended that the HCPC develop an anti-fraud policy and a fraud awareness programme. This could be delivered via eLearning.

- **Fraud Response:** HCPC does have a fraud response plan process map. However, there is no standalone fraud response plan policy – the fraud response process map, is linked to the Whistleblowing Policy. The Whistleblowing Policy does provide guidance on how to report concerns, but does not provide any detailed guidance on how investigations will be undertaken. Without clear guidance investigation may be mismanaged. For example, at the initial referral stage the fraud response process map includes a decision as to whether evidence needs to be isolated or duplicated but also needs to explain about the handling and maintaining the chain of evidence, as evidence may rendered inadmissible if handled incorrectly. This in turn may jeopardise any criminal prosecution or applications for recovering losses to fraud. Although, it is acknowledged that HCPC has access to trained investigators within the fitness to practise department who could advise on such matters. We have recommend that HCPC develop a fraud or serious incident response plan in order to address this weakness.

1.12 We also noted a potential area of improvement in relation to prevention and detection controls in respect of registrations. Registrants are not required to provide a DBS check (or relevant foreign police check) or proof of their right to work in the UK as part of the registration process. It was explained that DBS checks and right to work checks would be undertaken by the registrants' employer. However, some registrants operate as sole traders, therefore these checks will not be undertaken. Not undertaking such checks, particularly criminal records checks potentially exposes the public to safety risks. We have recommended that HCPC explore the possibility of undertaking such verifications as this would improve, already robust registrant due diligence procedures. It is acknowledged that as part of the registration process, applicants have to make a declaration as to whether they have any convictions or ongoing court cases. Where an applicant has made a declaration, these are passed onto Fitness to Practise in order to make a determination, where they will most likely compete a DBS check. However, if the applicant does not disclose that they have been convicted of a criminal offence (committing fraud by false representation), then the issue may not be detected via Registrations due diligence process.

Recommendations summary table

1.13 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	Strategic Approach to Managing Fraud	Amber	-	2	-
2	Fraud awareness	Red Amber	2	1	1
3	Prevention and Detection	Amber	-	2	4
4	Fraud Response	Amber	-	-	1
	Total recommendations made		**2**	**5**	**6**

1.14 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: Strategic Approach to Managing Fraud

Assessment: **Amber**

Background

The risk of fraud is an inherent risk to any organisation. As the most reported crime in the UK, accounting for more than 50% of all crime, it is essential that organisations understand the risk of fraud and to what extent they are exposed. By adopting a clear, strategic approach to managing the risk of fraud, ensures that the business remains proactive and agile in tackling the risk, developing a strong anti-fraud culture and less likely to fall victim to the emerging fraud risks. We reviewed the risk register and risk treatment plan and interviewed key members of staff to assess HCPC's approach to managing their fraud risk.

1.1 Heath & Care Professions Council's strategic approach to tackling fraud

Findings & implication

Positive findings

- The risk of fraud (and bribery) is included within the Risk Register and Risk Treatment Plan, for example, with the risk of bribery featuring on the corporate risk register and fraud risk is included on the finance and registrations risk registers. The register is reviewed by the senior management team (SMT) every six months. The inclusion of fraud and bribery ensures that the risks are being actively monitored.
- HCPC has service level agreement with NHS Counter Fraud Authority (NHS CFA) and a memorandum of understanding with NHS Scotland Counter Fraud Services (NHS SCFS). The agreements outline how both counter fraud services will provide support to HCPC in the event a registrant is subject to a fraud investigation. Furthermore, NHS CFA has also undertaken proactive exercises on registrant data in order to detect fraud, though the last proactive review was undertaken in 2015.
- Interviews with senior staff confirmed that there is an awareness of the specific fraud risks they are likely to encounter. For example, in respect of fitness to practise, there is a clear understanding and appreciation of the risk of conflicts of interest of people involved in the process. In being aware of the fraud risks, each area has been able to determine whether the controls in place for mitigating the risk of fraud are appropriate.

Recommendation

1. In order to adopt a more strategic approach to managing fraud risk, it is advised that the risk of fraud is more explicitly referenced within the strategic risk register. This will ensure that the risk of fraud is more effectively monitored and demonstrate a clear tone from the top. HCPC may wish to consider adding the risk of fraud as a separate risk within the register or adding fraud risk with the description of either risk 1 or risk 3.
2. It is recommended that specific fraud risks are included within relevant risk registers, and that they are subject to regular review - for example adding the risk of fraud to the corporate risk register.

Both Priority 2

Management response

Findings & implication

- The internal audit plan covers areas where fraud may be an issue/consideration – for example audits of finance and procurement cover fraud issues. Having an impartial assessment of internal controls ensures that they are operating effectively and that HCPC is not exposed to financial loss due to fraud or error.

Areas for improvement and implication

- The risk of fraud is not specifically included, or referenced within the strategic risk register, which is reviewed by the audit committee on a quarterly basis. The lack of an explicit reference may result in the risk of fraud not being specifically assessed – thus giving the Council false assurance that the risk is being effectively managed. It should also be noted that the audit committee last reviewed the entire Risk Register and Risk Treatment Plan (which does include fraud and bribery more explicitly) in November 2017.
- Although the risk of fraud (and bribery) is included within individual departmental risk registers, it was noted that there are some gaps and in some instances where there was not sufficient detail in relation to specific types of fraud HCPC is exposed to. For example, the risk of fraud is not explicitly included on the corporate risk register, whilst bribery is included. It is acknowledged that the financial impact of fraud would likely be low, however, the reputational damage in relation to a registration fraud would be high. As such, fraud is as a significant risk to HCPC and its absence from the corporate risk register may give the Council false assurance that the risk of fraud is being effectively managed across HCPC. Other registers where there are gaps include:
    - Finance risk register, where the risk is simply noted as the risk of fraud or theft. It does not distinguish between internal or external fraud as the modus operandi would differ greatly and therefore the controls to prevent those frauds would also be different.
    - Harm Register does not explicitly reference fraud, though does state harm by an incorrectly registered person. Harm caused by a fraudulent registrant should have specific consideration – this risk could be linked risk 10.2 on the Registrations risk register.

Recommendation

Recommendation1:

Accepted

Action: Risk of fraud has been added to the Strategic Risk Register commentary.

Action Owner: Chief Information Security and Risk Officer

Completion date: complete

Recommendation 2:

Accept

Action: As part of the next corporate risk register update, risk owners will be specifically asked if risk of fraud needs to be articulated within their risk areas.

Action Owner: Chief Information Security and Risk Officer

Completion date: January 2020

Key Risk Area 2: Raising fraud awareness

Assessment: Red Amber

Background

Research shows that raising fraud awareness within an organisation is one of the most effective controls in reducing internal fraud and a key driver in identifying and reporting external fraud. Raising fraud awareness can be achieved through various channels such as through training and through policies. Lack of focused training may result in staff not being able to identify fraud, or not knowing how to report their concerns (it is estimated that approximately 30% of identified fraud goes unreported). We reviewed policies and procedures and interviewed key members of staff in order to assess the fraud awareness regime within HCPC.

2.1 Raising fraud awareness (including training)

Findings & implication

Positive findings

- The Code of Conduct for Council Members makes good reference to conflicts of interest and the importance of raising concerns which may call into question ones actions. Furthermore, the Code of Conduct refers to the Nolan Principles, although not explicitly about fraud - it does reinforce HCPC commitment to conducting business in an ethical, open and honest manner.
- The Whistleblowing Policy makes reference to fraud as an example of a protected disclosure. Providing fraud as an example is best practice as it the criminal offence individuals are most likely to encounter.
- The Whistleblowing Policy also makes good reference to the Public Interest Disclosure Act 1998 and provides good clear guidance to staff, partners, and registrants, as to how they can report their concerns, directly and anonymously. Though the policy does encourage individuals to raise their concerns directly. This is best practice, as this anonymous reporting can make investigating issues more difficult. The Whistleblowing Policy also gives the reader the choice of reporting concerns externally to Public concerns at Work, which is best practice. It should be noted that Public Concerns at Work have rebranded and are now known as Protect.
- The HCPC website provides fitness to practise case studies, two of which are explicitly fraud related - timesheet/expenses fraud and fraud by abuse of position. Including such examples on the website is best practice and informs the public about the risk of fraud.
- The HCPC website banner (which is present on all HCPC webpages) has a link to reporting concerns, which is best practice. The employer reporting page does provide fraud as an example of a reportable concern.
- Staff within Registration and Fitness to Practise are provided with training which does cover elements of fraud. For example, in Registration, staff are made aware of the risk of individuals gaining access to the register using false information.

Recommendation

3. It is recommended that HCPC develop an Anti-Fraud Policy which clearly articulates HCPC's zero tolerance approach to combatting fraud and how to report concerns.

Priority 1

4. It is recommended that HCPC develop fraud awareness training to be completed by all staff. This could be in the form of e-learning.

Priority 1

5. It is recommended that Code of Conduct provides details of fraud and whistleblowing procedures. The Code of Conduct should also include links to those policies.

Priority 3

6. It is recommended that HCPC ensure that only one version of the Anti-Bribery Policy is available and that the Anti-Bribery Policy include more details as to how staff should raise their concerns. For example, the section should name an individual or job title to whom reports should be made to, as well as some alternative avenues. The reporting mechanism should be in line with whistleblowing reporting and the, to be drafted, Anti-Fraud Policy.

Priority 2

✖

Management response

Findings & implication	Recommendation
Areas for improvement & implication • HCPC does not have a fraud policy and there is no fraud awareness programme across HCPC, although there is a good level of fraud awareness amongst senior management interviewed. The risk of fraud is not covered at induction or as part of an annual refresher training. A lack of fraud awareness may result in staff not being able to detect or report instances of fraud, resulting in continued losses. Lack of awareness will also fail to discourage individuals from committing fraud. • The code of conduct, although makes good reference to conflicts of interest and the Nolan Principles; the code of conduct does not provide reference to fraud or whistleblowing. It is best practice for a code of conduct to refer to other related policies. • The Anti-Bribery Policy 2017 articulates HCPC's zero tolerance approach, provides a clear explanation as to what is bribery and the types of offences under the Bribery Act 2010, however, does not provide any guidance as to how staff can raise their concerns should they suspect someone is committing bribery. The policy simply states that staff must raise their concerns to the 'HCPC Secretariat' and the relevant paragraph is incomplete. Not providing a clear route to reporting concerns may result in issues going unreported, or matters being reported to inappropriate individuals. • We were provided with three versions of the Anti-Bribery Policy, the Anti-Bribery 2017, Anti-Bribery 2014, Anti-Bribery, Gifts and Hospitality Policy 2013 and Anti-Bribery, Gifts and Hospitality Policy 2012. Although all the policies do provide the same information, having too many versions available may cause confusion.	**Recommendation 3:** **Accept** **Action: The HCPC's policies will be updated as recommended. It is aimed that these be presented to Council in December 2019 for approval.** **Action Owner: Chief Information Security and Risk Officer & Interim Director of HR and OD** **Completion date: December 2019** **Recommendation 4:** **Accept** **Action:** E learning will be developed by the Learning and Development team in conjunction with the Chief Information Security and Risk Officer, who will assume central oversight of fraud policy and awareness. **Action Owner: Chief Information Security and Risk Officer** **Completion date: Q4 FY19/20** **Recommendation 5 and 6:** **Accept** **Action:** The HCPC's policies will be updated as recommended. It is aimed that these be presented to Council in December 2019 for approval. **Action Owner: Chief Information Security and Risk Officer & Interim Director of HR and OD** **Completion date: December 2019**

Key Risk Area 3: Prevention and Detection

Assessment: Amber

Background

An essential element of an organisations counter fraud strategy is ensuring there are mechanisms in place for preventing and detecting fraud – the most effective of which being those which require approvals. However, an organisation needs to strike a balance between operational effectiveness and preventing fraud, hence there needs to be a risk based approach tailored to the organisation. We reviewed policies and procedures and interviewed key members of staff in order to gain an understanding of key anti-fraud controls within Finance, Procurement, Human Resources, Registrations, Fitness to Practise and IT.

3.1 Finance - As with most businesses, the finance function is often in a unique position to access the accounting and banking systems which makes them a prime target for fraudsters. It is therefore important that there exists strong key financial controls for preventing and detecting fraud. The controls have not been tested for operational effectiveness, only the principle design has been considered.

Findings & implication

Positive findings

- Bank mandate and CEO fraud remains a significant threat to all organisations. Finance has responsibility for processing changes to the bank mandates of suppliers. This requires the supplier to confirm any changes to bank mandates on headed paper and this is followed up by a telephone call (using a noted contact within Sage) to confirm the change. Once confirmed the change is approved.
- The finance department is subject to regular internal audits, such as key financial controls audits. Fraud risk is a consideration as part of the audits. The regular auditing of finance ensures that controls for preventing fraud and error are designed and operating effectively.
- Finance use Sage accounting system to manage workflow. This system is limited to relevant finance staff and enforces segregations of duties. For example a member of staff cannot approve a payment which they have created. This is a robust control for preventing internal fraud.
- Journals are only posted once they have been approved by the Head of Financial Accounts. This also, is an effective control in preventing false accounting in order to conceal another fraud.
- Finance (as well as Human Resources) will undertake verification of payroll (which is delivered by a third party provider) before it is approved for payment. A variation report will be reviewed in order to identify and scrutinise any changes from the previous month and confirm they are genuine variations. This is best practice and reduces the risk of ghost employees or leavers remaining on payroll and thus receiving a wrongful credit.

Areas for improvement & implication

- Although staff are provided with specific training on how to use the accounting systems etc., there is no specific training in relation to fraud. Although, the residual risk of fraud to finance is

Recommendation

7. HCPC should consider developing finance specific fraud awareness training to be included within the finance induction training. This will make staff more aware of the risk of fraud and more likely to report any concerns.

Priority 3

✓

Management response

Accept

Action: The Learning and Development team will assist the Finance Department in developing fraud specific induction material.

Action Owner: Interim Director of Finance

Completion date: Q4 FY19/20

Findings & implication	Recommendation
considered low, due to the key financial controls, fraud could be successfully committed through unknown methods or if a fraudster can convince staff within finance (through deception or coercion) to bypass certain controls.	

3.2 Procurement - Procurement is normally the second most targeted area for fraud and bribery and can also be the most difficult to detect. Having a clear workflow for managing tenders is important for preventing procurement fraud. Additionally, it is important for organisations to implement controls post contract award. Not only does this ensure that value for money is obtained but also prevents suppliers charging for services not delivered. We reviewed the Procurement Policy and interviewed the Finance and Procurement Officer and Interim Finance Director. The controls have not been tested for operational effectiveness, only the principle design has been considered.

Findings & implication

Positive findings

- HCPC has a purchase order system, WAP with an electronic Scheme of Delegation coded into the system. As such the same user cannot raise and approve the same purchase order. In having a purchase order system, finance can not only more effectively monitor expenditure but also prevent false invoicing and identify/challenge any irregularities before payments are committed.
- There is a clear process for conducting a tender. When conducting a tender, procurement will ensure that the budget holders and end users are involved in the process of drafting the requirement, assessing and evaluating the bids. This ensures that the best bidder is awarded the contract thus reducing the risk of a supplier defrauding HCPC. Additionally, value for money is the primary consideration when awarding contracts, this ensures that bidders cannot deliberately make unrealistic bids in order to win the contract.
- Procurement undertake due diligence on bidders in order to confirm they are genuine and have the financial stability to deliver the contract.
- Single tender waivers are tightly controlled by HCPC and only made in exceptional circumstances. It was explained that HCPC would typically have no more than two single tender waivers per year and this would require the approval of the Director of Finance and the CEO to proceed.
- The Procurement Policy places importance on declaring conflict of interest, referencing the Bribery Act 2010, Anti-Bribery, Gifts and Hospitality Policy. All persons involved in a procurement are required to declare any conflicts of interest. This is best practice and maintains the integrity of the process.
- When engaging in large projects HCPC will engage with third parties and specialists in order to gain additional assurance. For example with respect to construction projects, HCPC will engage an independent quantity surveyor in order to provide them with assurance that the project is being delivered. Not only does this ensure HCPC can achieve value for money, but will also deter contractors from deliberate underperformance (fraud by false representation) in order to improve profitability.

Areas for improvement & implication

Recommendation

8. It is recommended that budget holders receive training about the fraud risks associated with contractors. This training could be delivered via eLearning and potentially included within general fraud awareness (see recommendation 4).

Priority 3

✓

Management response

Accept

Action: E learning will be developed by the Learning and Development team in conjunction with the Chief Information Security and Risk Officer, who will assume central oversight of fraud policy and awareness.

Action Owner: Chief Information Security and Risk Officer & Interim Director of HR and OD

Completion date: Q4 FY19/20

Findings & implication	Recommendation
- Although budget holders are provided with some training on how to manage contracts there is not specific fraud consideration within the training. A lack of awareness of the fraud risks associated with procurement may result in fraud going undetected or unreported.	

3.3 Human Resources - Research conducted by the Office of National Statists and CIFAS have identified that 71% of Fraud is committed by internally by employees. Therefore, it is important that controls in place for vetting, training and on-boarding employees are robust in mitigating the risk of Fraud and identifying unsuitable candidates. We reviewed the recruitment procedures and interviewed the HR Business Partner. The controls have not been tested for operational effectiveness, only the principle design has been considered.

Findings & implication

Positive findings

- The Recruitment Policy provides guidance on interviewing candidates, specifically it states that at least one of the interviewers on the panel need to be a trained interviewer. Having trained interviewers not only ensures that inappropriate candidates are identified at the interview stage. Additionally, the policy states that some roles may require a DBS check.
- HCPC uses an HR management system CoreHR. Using such a system maintains a robust audit trail and will enforce segregations of duties within HR. As such the risk of ghost employees is significantly reduced as new employees require management approval before they are fully added to CoreHR and subsequently to the payroll (which is outsourced).
- HR is responsible for updating the standing data for payroll. Input checks are conducted on the starter, leaver and pay changes reports on a monthly basis before they are sent to the payroll provider. Before payroll is processed for final payment, HR (in addition to finance) will verify payroll. For example, HR will confirm new starters and leavers have been included and removed accordingly. This control also significantly reduces the risk of ghost employees being added to payroll.
- There is a self-service process for employees to make changes to personal details. Using self-service is best practice and ensures that staff bank accounts cannot be changed by individual members of staff in HR on instruction from a fraudster posing as the member of staff.

Areas for improvement & implication

- As part of the recruitment procedures, HR will undertake due diligence on the candidate - including reference checks and verify passports – which is best practice. However, these procedures are not outlined within the Recruitment Policy.
- As part of the risk assurance mapping review, it was identified that HR had not been subject to an internal audit review in recent time. Internal audit reviews are essential for establishing whether key controls are operating effectively.

Recommendation

9. It is recommended that the candidate vetting procedures are outlined within the Recruitment Policy.
10. It is recommended that an internal audit review is undertaken in the area of HR in order to assess the effectiveness of the key controls.

Both Priority 3

✓

Management response

Recommendation 9:

Accept

Action: Vetting procedures will be outlined in the recruitment policy.

Action Owner: Interim Director of HR and OD

Completion date: Q3 FY19/20

Recommendation 10:

Accept

Action: BDO proposed a review of HR in its three year audit strategy. The Executive welcomes this review should it be prioritised by the Audit Committee as part of the 2020-21 Internal Audit Plan.

Action Owner: BDO

Completion date: For Audit Committee to prioritise

3.4 Registration - The process for registration needs to be robust and controls need to be in place for identifying individuals seeking to obtain registration fraudulently as there is a significant risk to the public. We interviewed the Head of Registration. The controls have not been tested for operational effectiveness, only the principle design has been considered.

Findings & implication

Positive findings

- The Registration team work to a standard operating procedure which includes specific due diligence checks which must be performed. For example the Registration team has access to Keesing, a database which assists with identifying valid types of documentation from countries worldwide.
- References are verified by the Registration team and if necessary, HCPC will go back to the referee in order to confirm veracity of the reference. Additionally, HCPC will also contact the counter signatories of documents in order to confirm the counter signed document is genuine.
- The Registration team undertake quality checks of registrant files in order to confirm they are complete. This provides assurance to HCPC that processes are operating effectively and will prevent fraudsters from gaining access to the register.
- There are no set specialisms within the Registration team due to the changing demands on the department. Members of the team may be answering phones one day and then will be processing a registration request the following day. Registrations are processed as they are received, though there is no control as to who in the team they are assigned to; furthermore, no one member of staff will complete the entire registration process. This reduces of fraudulently processing an application.
- As previously noted, NHS Counter Fraud Authority has undertaken proactive exercises on registrant data in order to detect fraud, although the last proactive review was undertaken in 2015.
- The Registration team will verify qualifications with the institutions (domestic and foreign). International applications are each assessed by two partners from the relevant part of the Register to ensure the education and experience meets the required standards. At least one registrant from the same area of the register on the clinical side and one from the academic side of the profession are involved (on behalf of HCPC) in the process. Any details provided during the application process of membership of a professional body or registration with a regulator is also checked as part of the verification process, this reduces the risk of unqualified or under qualified individuals becoming registered and potentially posing a risk to the public.
- There is a risk of conflicts of interest when assessing the quality of another UK qualification. It was explained by HCPC that competition in the market may mean that, for instance, that an academic is assessing a course which is in competition with their own, thus raising a conflict of interest. This risk is managed through the requirement of Partners having to declare interests and the report is

Recommendation

11. It is advised that HCPC explore whether, legislatively, they can perform criminal records (on registrants who have completed a non-UK Approved Programme) and right to work checks on registrants.
12. It is advised that HCPC consider introducing photographic ID cards as an added layer of assurance. Alternatively, HCPC may wish to consider adding the registrants' photo on the website, though it is acknowledged this may not be practicable.

Both Priority 2

✓

Management response

Recommendation 11:

Accept

Action: HCPC will explore, legislatively, and if there are potential benefits.

The costs of undertaking criminal record and right to work checks for c.370,000 registrants would be have a significant impact on the HCPC's budget. The human resource required to manage the check system (including renewal of checks) would also be considerable. These additional steps in the registration process would also lengthen registration processing times.

The legal feasibility of this will be explored, as well as the current practise of other regulators. If this is legally possible (and desirable taking the above into account) consideration would be needed as to if the cost the check can be passed onto the applicant/registrant.

Action Owner: Head of Registrations

Findings & implication	Recommendation
drafted by the Education Officer which needs to be agreed by Panel member and approved by the relevant committee. These segregations of duties and multiple stages of review ensure that any biases would most likely be detected. **Areas for improvement & implication** • Registrants are not required to provide a DBS check (or relevant foreign police check) or prove they have the right to work in the UK as part of the registration process. It was explained that DBS checks and right to work checks would be undertaken by the registrants' employer. However, some registrants operate as sole traders, therefore these checks will not be undertaken. Not undertaking such checks, particularly criminal records checks, could potentially expose the public to harm. It is acknowledged that as part of the registration process, applicants have to make a declaration as to whether they have any convictions or ongoing court cases. Where an applicant has made a declaration, these are passed onto Fitness to Practise in order to make a determination, where they will most likely compete a DBS check. Additionally, for UK Approved Programme, students are required to pass an enhanced or equivalent criminal records check prior to commencement. Where there is a registrant commits and offence the UK Police inform HCPC. However, if the applicant, who has completed a non-UK Approved Programme, does not disclose that they have been convicted of a criminal offence (committing fraud by false representation), then the issue may not be detected via Registrations due diligence process. • It ws noted that registrant ID cards are no longer issued and are now only issued a with certificate of registration. The lack of photographic identification means that the public will not be able to easily confirm the ID of the registrant. The lack of photo may result in a registrant giving/sharing their details fraudulently to other non-registered individuals so they can practice - this risk would most likely occur with sole traders. In discussions with the Head of Registrations, there have been no such reported cases and it is acknowledged that a photo ID would not eliminate the risk, it would primarily deter potential fraudsters.	**Completion date: Q4 2019-20** **Recommendation 12:** **Reject** **Action:** Registrant cards were discontinued a number of years ago as part of efforts to streamline costs. These were not ID cards as they were only be valid from the day of issue and could be easily replicated. Reintroduction of the cards, including a photo, is not recommended at this time, given the costs and limited value as an anti-fraud mitigation. However registration cards will be explored as a 'value add' service as part of the accelerated strategic priority programme. **Completion date: N/A**

3.5 Fitness to Practise - is an essential process for protecting the public from individuals who are not fit to practice. The process for handling fitness to practise investigations need to be robust in their approach and evidence based. We interviewed one of the Department Leads for Fitness to Practise and reviewed the Case Management Manual. The controls have not been tested for operational effectiveness, only the principle design has been considered.

Findings & implication

Positive findings

- The fitness to practise department work to the Case Management Manual (the Manual is still subject to final sign off). The Manual makes reference to fraud throughout the document. For example as one of the ways in which a registrant may harm someone or employer. The Manual also provides the contact details of the NHS CFA, NHS SCFS and NHS Counter Fraud Services Wales.
- Where a registrant is suspected of fraud and is in the employ of the NHS, HCPC will allow the bodies Local Counter Fraud Specialist (or NHS CFA) to lead/conduct the investigation. The reason being that the Local Counter Fraud Specialist will have better access to information and has local knowledge, which will help expedite an investigation.
- The Fitness to Practise team use Charter as their case management system. User have unique logins and access is regularly reviewed. The system does not allow for cases to be deleted and changes are fully auditable.
- Decisions to not open a formal investigation at the point of triaging a referral will be subject to management review. Having management oversight ensures that referrals are not dismissed due to error, fraud and/or corruption.
- Fitness to Practise have a quality compliance framework whereby they undertake quality reviews on cases to ensure that they meet the required standard.
- Fitness to Practise is for the most part paperless and all records are stored on Charter. Where there is a need to store physical evidence, Fitness to Practise have an evidence locker which is locked and evidence is logged in and out. Maintaining the chain of custody of evidence is imperative for successful investigations.
- Partners are adjudicators at fitness to practise hearings. Partners are required to make declarations of interest if they are conflicted at a hearing. Additionally, Partners are randomly selected from around the UK and cannot sit on multiple hearings in relation to same case– i.e. if the Partner sits on the first hearing, they cannot sit on the final hearing. This process maintains the transparency and integrity of the hearing.

Areas for improvement & implication

- None noted.

Recommendation

None

✓

Management response

N/A

3.6 IT - Fraud is now primarily committed via the internet and IT systems, this is because it provides the fraudster with distance from the victim and a semblance of anonymity. Although cyberattacks may not be a fraud in the first instance, the data they attempt to extract is generally used in the pursuit of fraud. For example personal information is used to create false identities. Organisations, therefore, need to ensure that they have the right controls in place for securing their own data and preventing unauthorised access. We interviewed the Infrastructure Manager in IT. The controls have not been tested for operational effectiveness, only the principle design has been considered.

Findings & implication	Recommendation
Positive findings • The IT department has been subject to numerous audits from external parties in order to assess the effectiveness of IT controls. Audits include a Cyber Security review by Grant Thornton in 2018 as well as numerous audits in relation to obtaining the ISO27001 certificate. • Penetration tests are undertaken on a quarterly basis in order to establish whether the controls are operating effectively. • HCPC is in the process of transferring social worker registrant data to Social Work England, who will take responsibility of social workers from 2 December 2019. The IT department risk assessed their options for transferring the data, from transferring the data using external hard drives to using cloud services. Following a risk assessment, the IT team are going to transfer the data using Microsoft Azure Blob storage, where Social Work England will be the administrator as they will be the ultimate data controller. • There is a data exchange agreement between HCPC and Social Work England outlining the agreed process and roles and responsibilities. The data will be encrypted at rest, where it will be then transferred into Microsoft Azure Blob storage. Access to the storage area is secured by two factor authentication. Once the data has been transferred, HCPC will request that access to the area is removed immediately. Areas for improvement & implication • None noted	None ✓ **Management response** **N/A**

Key Risk Area 4: Hold to Account

Assessment: **Amber**

Background

When issues are identified and reported it essential for an organisation to have a clearly defined process for conducting investigations. The lack of a process risks issues not being handled in a timely manner and poor decision making resulting in continued losses, both financial and reputational. We interviewed the Head of Compliance and reviewed key policies and procedures. The controls have not been tested for operational effectiveness, only the principle design has been considered.

4.1 Hold to Account

Findings & implication

Positive findings

- HCPC has a process map outlining how HCPC will respond to a reported fraud. The process map provides clear steps which need to be followed. Having a response plan is best practice as it ensures that the investigation commences in a timely manner, reducing the risk of further losses.
- In the event that an internal investigation needs to be conducted, HCPC will use Fitness to Practise staff, where appropriate, to assist as they are experienced investigators. Having trained individuals investigating ensures that processes are followed and avoids the integrity of the investigation being called into question.

Areas for improvement & implication

- There is no standalone fraud response plan policy – the fraud response process map, is instead linked to the Whistleblowing Policy. As previously noted, the Whistleblowing Policy does provide guidance on how to report concerns, however, does not provide any detailed guidance on how investigations will be undertaken. For example, at the initial referral stage the fraud response process map includes a decision as to whether evidence needs to be isolated and or duplicated. Although in general this is good practice, there may also need to be a consideration about handling evidence, as it may render it inadmissible, which may jeopardise any criminal prosecution or applications for recovering losses to fraud. It is acknowledged, however, that HCPC has access to trained investigators within the fitness to practise department who could advise on such matters.

Recommendation

13. It is recommended that HCPC develop a fraud response plan policy, or serious incident response plan. The procedure should provide detailed guidance about each stage of the investigation – mirroring the fraud response plan map.

Priority 3

✓

Management response

Accept

Action: This will be included in the revised harmonised fraud policy as outlined in recommendations 3, 5 & 6.

Action Owner: Chief Information Security and Risk Officer & Interim Director of HR and OD

Completion date: Q4 FY19/20

A Audit objectives, Risks & Scope

Terms of reference	
Objectives	The objective of the audit is to provide assurance to the HCPC that they have robust controls to prevent, deter and detect fraud.
Key risk areas	• The HCPC's strategy for managing their fraud risk is appropriately designed; and • There are adequate controls in place for preventing, deterring and detecting fraud (specifically within the main fraud risk areas).
Scope	In order to effectively manage the risk of fraud, an organisation needs to create an anti-fraud culture. This is achieved through implementing the four pillars of good fraud risk management: (a) clear strategic approach to combatting fraud; (b) raising awareness amongst staff and stakeholders; (c) implementing controls to prevent; and (d) deter fraud and having a regime for detecting and investigating fraud. Therefore in order to provide an assessment of HCPC's approach to combatting fraud we will review the four pillars and provide guidance and recommendations in relation to:Strategic Governance in tackling fraud; • Culture, training and Raising Concerns; • deterrence and prevention (e.g. effective control systems); and • detection and investigation.
Approach	The audit will be split into two sections that will cover the strategic governance, culture, raising concerns, prevention, detection and training. The review will be undertaken as follows: • **Section 1 - Counter Fraud Policy Review:** HCPC's fraud related policies will be reviewed from a counter fraud perspective to ensure that they are fit for purpose and in line with current legislation. • **Section 2 - Fraud Risk Assessment:** The fraud risk assessment will be undertaken into areas of the business that are most exposed to the risk of fraud, adopting a risk based approach. The review will involve meeting with the key members of staff for each proposed area and review specific policies, procedures and awareness in order to determine whether the anti-fraud controls and framework is adequate, proportionate and fit for purpose. It will also include assessing the adequacy of segregations of duties and the integrity of processes to ensure they are as fraud proof as possible. Where areas of improvement are identified in respect of HCPC's counter fraud arrangements, we will make recommendations in order to address those weaknesses. It is proposed that the following areas should be assessed from a high level and will not involve any substantive testing: – Procurement department – Human resources & Payroll – Finance – Registration – Fitness to Practise – IT

B 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.

C Staff consulted during review

Name	Job title
Suellen Vassell	**Financial** Accountant
Gordon Dixon	Interim Finance Director
Antonio Pinheiro	Finance and **Procurement** Officer
Ben Spittles	HR Business Partner
Richard Houghton	Head of **Registration**
Sarita Wilson	Department Lead - Case Reception and Triage. **FTP**
Jason Roth	Infrastructure Manager, **IT**
Roy Dunn	Chief Information Security and Risk Officer

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

FOR MORE INFORMATION:

SARAH HILLARY

+44 (0)20 7651 1347
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.