Audit and Risk Assurance Committee

14 June 2023

Internal Audit – Annual Report and Opinion

Executive Summary

The annual opinion is reached through a risk-based plan of work, agreed with management and approved by the Audit and Risk Assurance Committee. This should provide a reasonable level of assurance, subject to the inherent limitation of internal audit (covering both the control environment and the assurance over controls).

The audit opinion takes together the assurance ratings and recommendations of individual assignments conducted in 2022-23, management's responsiveness to internal audit recommendations and the direction of travel with regard to internal control, governance and risk management.

Previous consideration	Annual standing report. The report has been reviewed by ELT.
Decision	The Committee is invited to discuss the report.
Next steps	N/A
Strategic priority	All
Risk	There is some risk that management's objectives may not be fully achieved. Improvements are required in those areas to enhance the adequacy and effectiveness of governance, risk management and internal controls.
Financial and resource implications	The cost of the annual report is included in the Internal Audit annual fee.
Author	BDO LLP

INTERNAL AUDIT ANNUAL REPORT

2022/23

HEALTH & CARE PROFESSIONS COUNCIL

CONFIDENTIAL
STATUS – DRAFT V03

JUNE 2023

BDO

Contents

Document history		Distribution	
Draft v03	02/06/2023	Health & Care Professions Council	Draft v3

Author: William Giffin
Heather Buckingham & Dan Bonner

Reviewed by: Bill Mitchell

1. Executive Summary & Opinion

Introduction

1.1 The International Professional Practices Framework (IPPF) and the associated International Standards for the Professional Practice, provide the basis of internal auditing standards in the UK. They state that the Head of Internal Audit is required to produce an annual report on the risk management, governance and control framework on the organisation subject to internal audit.

1.2 The UK Public Sector Internal Audit Standards (PSIAS), to which we work to, also require the Head of Internal Audit to provide a formal annual opinion to the Accounting Officer, providing assurance on the effectiveness of the organisation's risk management, control and governance processes. Given HCPC's role and external auidt by the National Audit Office, we also adhere to PSIAS.

1.3 Standards also requires the Head of Internal Audit to provide a summary of the internal audit work undertaken across the year, which can be used support Health & Care Professions Council Governance Statement. This report thus:

- provides assurance to the Accounting Officer on areas reviewed, to support the Governance Statement, which is included in Health & Care Professions Council annual report and accounts;
- summarises internal audit activity in 2022/23;
- highlights the assurance ratings and key issues arising from the individual reviews undertaken in the year; and
- confirms compliance with the IPPF and PSIAS.

1.4 While this report and annual Internal Audit Opinion is a key element of the framework designed to inform the Annual Governance Statement, there are also a number of other important sources of assurance which the Accounting Officer utilises.

Scope

1.5 The annual opinion is achieved through a risk-based plan of work, agreed with management and approved by the Audit, Risk and Assurance Committee, which should provide a reasonable level of assurance, subject to the inherent limitation of internal audit (covering both the control environment and the assurance over controls) described below and set out in Appendix D. The opinion does not imply that Internal Audit have reviewed all risks relating to the organisation. We experienced no limits to the scope of our audit work.

Internal Audit Annual Opinion

1.6 The audit opinion takes together the assurance ratings and recommendations of individual assignments conducted in 2022/23, management's responsiveness to internal audit recommendations and the direction of travel regarding internal control, governance and risk management. Our opinion is MODERATE that:

1.7 ***There is some risk that management's objectives may not be fully achieved. Improvements are required in those areas to enhance the adequacy and effectiveness of governance, risk management and internal controls.***

1.8 This is a 'level 2' or MODERATE opinion of four rating levels. This year's opinion is improved compared to the previous year, where HCPC have received a 'level 3' or LIMITED rating. The main reason for the improved rating is that strong improvements have been made to financial controls. In 2021/22, we reported a RED or NO ASSURANCE report on financial controls. In 2022/23, as part of our 2022/23 follow up work, we re-rated the finance area as MODERATE, reflecting

the hard work HCPC had put in since the original audit findings were confirmed. Furthermore, most of our other audit reports this year, we assigned a MODERATE rating overall.

1.9 We also note that HCPC has made a conscious effort to improve its control environment in terms of implementing recommendations. Although most notable in the finance area, other areas of the organisation have also seen a closure of important recommendations. Not only does it self-review implementation progress, out of 12 previous audit recommendations made, we noted that seven recommendations have been fully implemented and five partially completed. To further support the implementation of recommendations and thus the robustness of HCPC's overall control framework, HCPC has had a focus on its second line assurance function which has matured.

1.10 We note that the second line of assurance has found similar levels of assurance as ourselves.

1.11 The basis for the opinion is given in the next section (Section 2), with a summary of the findings from our assurance work is in Section 3

2. Basis for the annual opinion

Introduction

2.1 The annual opinion is drawn mainly from the results and assurance ratings stated in our individual audit reports. Our opinions for each assignment are based on our assessment of whether the controls in place support the achievement of management's objectives as set out in our individual assignment terms of reference.

2.2 We also consider other factors in forming our annual opinion, including the:

- responsiveness of management to the implementation of our audit recommendations during the year;
- results of any other relevant work such as advisory assignments, investigations and special exercises conducted by ourselves, management or third parties, where applicable; and
- the direction of travel of the effectiveness of the organisation's internal control, governance and risk management processes.

Individual Assignment Assurance Ratings

2.3 Overall, there were seven audit assignments conducted during the year including a general follow up review. The pie chart (Figure 1a) summarises the assurance opinions provided in six audits undertaken (FtP is still in draft) and Figure 1b shows the number of recommendations therein, by priority rating. There were no advisory assignments conducted during the year. We reviewed design only for the Cyber review.

2.4 Our initial draft reports are sent to the key officer responsible for the area under review to gather management responses and develop an action plan. In every instance, there is an opportunity to discuss the draft report in detail. Therefore, any issues or concerns can be discussed with

Figure 1a. Summary of Assurance Report Ratings for 2022/23

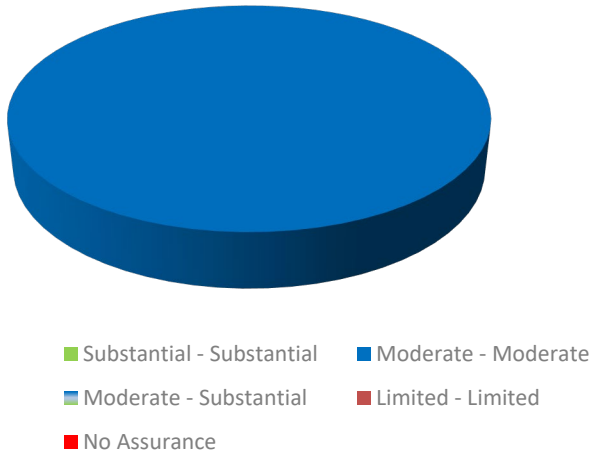
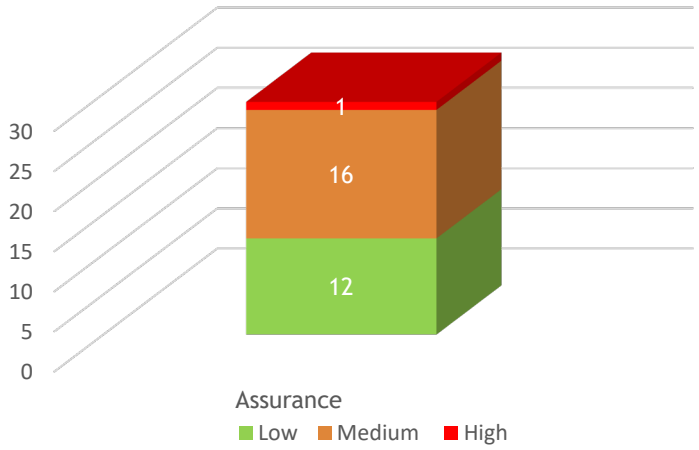


Figure 1b. Summary of Recommendations Priority Ratings Raised in 2022/23.



management before finalisation of the reports and recommendation and their due date for implementation is agreed with management.

Significant Findings Affecting the Opinion

2.5 It is a requirement of internal auditing standards to highlight any significant issues identified during the year identified in our work and for management to include them in the Governance Statement. We have no areas of significance to raise this year.

Effects of any Significant Changes in Organisational Objectives or Systems

2.6 As we reported in our Annual Report in the previous two years, HCPC were able to maintain governance, risk management and internal control processes while retaining several systems and processes to a virtual environment, migrate to a hybrid working model and a return to a physical offering at the Kennington site. A hybrid model is still in place and is now successfully operating as 'business as usual'.

Significant Matters Arising from Previous Internal Audit Reports

2.7 There were specific matters arising from previous internal audit reports that might have had an impact on our annual opinion for this year. Our work in the previous year identified significant issues in Finance and as a result HCPC received a 'RED' or 'NO ASSURANCE' report, with seven High and three Medium findings. That said, we completed a full follow-up on Finance, 're-testing' all areas covered in the previous report and provided a 'MODERATE/MODERATE' rated report, with two Medium and two Low priority findings. The two Medium findings related to:

a. policies and procedures were not up to date and remain difficult to navigate and maintain because they comprise over 116 documents.

b. lack of documented evidence to demonstrate a segregation of duties for approvals of changes of supplier bank details.

2.8 Both recommendations are due to be implemented by the end of September 2023.

Table 1: Assurance ratings for all audit plan assignments conducted 2022/23

Assignment	Design Effectiveness	Control Effectiveness	Recommendations Priority rating		
			High	Med	Low
1. Unified Assurance Framework	■	■	-	3	1
2. Diversity	■	■	-	1	4
3. Registrant Forecasting	■	■	1	4	3
4. Key Financial Controls - Follow up	■	■	-	2	2
5. Cyber Security	■	■	-	5	-
6. Fitness to Practice*	■	■	-	1	2
7. Follow up*	■	■	-	-	-
TOTAL for 2022/23			**1**	**16**	**12**

** Report is in draft and so the opinion and number of recommendations have not been confirmed.*

Responsiveness to internal audit recommendations

2.9 A critical part of an organisation's internal control, governance and risk management framework is management's responsiveness to the implementation of agreed internal audit recommendations. Timely and full implementation of internal audit recommendations indicates that management are making positive steps towards improvement.

2.10 Health & Care Professions Council monitors the implementation of recommendations and reports the outcome of the implementation process to the Audit, Risk and Assurance Committee. Internal Audit reviews the implementation of recommendations as part of the work conducted for individual assignments where the assignment covers areas of work subject to previous internal audit recommendations. Moreover, Internal Audit selects a sample of higher and medium priority recommendations to verify with recommendations have been implemented as agreed.

2.11 We sampled 12 medium priority recommendations, due to be implemented by 31 December 2022 or before, covering the following audits: Intelligence Gathering (20/21), Financial Modelling (20/21), Safeguarding (2021/22, Education (2021/22) Registration Payments Processes (2021/22) and IT Cyber (2023/23). A full follow up was completed for the Key Financial Controls (2021/22) review whereby the audit identified several improvements had taken place and were due to take place resulting in an improved level of assurance of MODERATE/MODERATE.

2.12 We found that of the 12 recommendations were followed up on, seven were implemented and four were either partly or not yet implemented. One was superseded and closed. Given that all recommendations partly implemented were found to be well progressed and had agreed extension dates for this year, we consider that a Moderate rating is appropriate.

2.13 No high priority recommendations were due to be implemented by 31 December 2022 that we have not already followed up on previously.

Direction of travel

2.14 We have provided some analysis of our opinions over the last three years. Our assurance ratings are an assessment at the time the assignment was conducted. However, organisations rarely remain static – the internal control, governance and risk management in an organisation may improve or deteriorate in individual areas or across the whole organisation over time.

2.15 One indicator of the direction of travel is the assurance rating and number of recommendations per assignment between the current year and previous years. While assignment subjects differ each year and thus coverage to what the assurance ratings refer, such a comparison can give an indication of the direction of travel for an organisation.

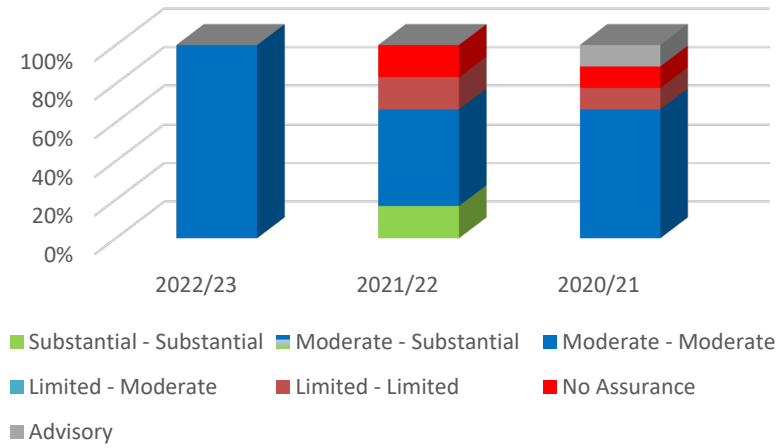
2.16 We have also compared the audit report 'traffic light' opinions over the last three years and the associated priority rating of recommendations. This is shown in Figure 2a and 2b overleaf, in absolute numbers.

2.17 The graphs give a broad indication of the direction of travel for audit assignments' assurance ratings.

2.18 We have continued to balance assurance and advisory assignments across the Plan to enhance the value that Internal Audit brings to HCPC, and we continue to engage subject matter experts to undertake reviews in specialist areas where they can add further value to the assurance provided to HCPC and the Audit, Risk and Assurance Committee.

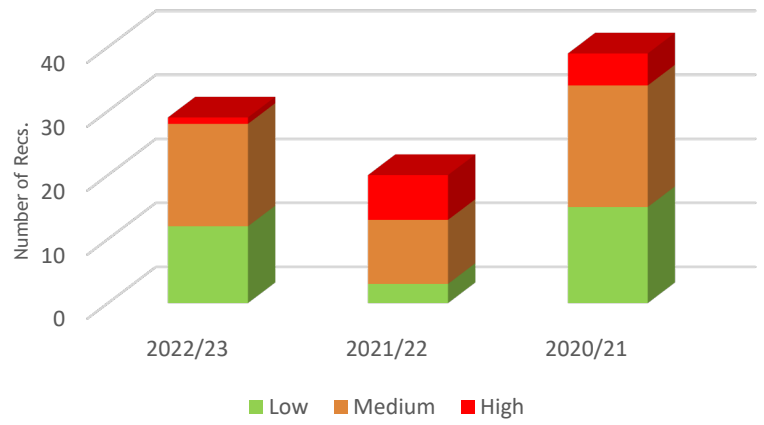
2.19 Furthermore, Figure 2b provides an assessment of the number and priority of audit recommendations raised in our reports. However, it is not possible to draw a direct comparison across the three years as the areas of focus differs year on year and so does the associated risk. Some areas by nature lend to more risk and thus a higher proportion of recommendation.

Fig. 2a Report Assurance Ratings 2020/21 to 2022/23



Opinion	2022/23	2021/22	2020/21
Substantial - Substantial	-	1	-
Moderate - Substantial	-	-	-
Moderate - Moderate	7	3	6
Limited - Moderate	-	-	-
Limited - Limited	0	1	1
Red - Red	-	1	1
Advisory	-	-	1

Figure 2b. Recomendations by priority - 2020/21 to 2022/23



Opinion	2022/23	2021/22	2020/21
High	1	7	5
Medium	16	10	19
Low	12	3	15

Completion of the audit plan

2.20 Internal audit work was performed in accordance with BDO Internal Audit methodology which conforms to the Public Sector Internal Audit Standards and Chartered Institute of Internal Auditors' Position Statement on Risk Based Internal Auditing. The Public Sector Internal Audit Standards require the annual report to include the results of the Internal Audit function's quality assurance and improvement programme. Details of our method and quality assurance programme are outlined in Appendix C.

2.21 Our findings are based upon and limited to the results of the internal audit work performed during the 2022/23 financial year. In completing the delivery of our audit plan, there were no restrictions placed upon the scope of our work.

Table 2: Internal Audit assignments conducted in 2022/23

Assignment	Work type	Completion status
Unified Assurance Framework	Assurance	Complete
Diversity	Assurance	Complete
Registrant Forecasting	Assurance	Complete
Key Financial Controls - Follow up	Assurance	Complete
Cyber Security	Assurance	Complete
Fitness to Practice*	Assurance	Draft
Follow up*	Follow up	Draft

APPENDIX A – Summary of High & Medium Priority Recommendations

Priority	Findings & *Recommendations*		
Unified Assurance Framework (UAF)		**MODERATE (DESIGN)**	**MODERATE (EFFECTIVENESS)**
Medium	**We examined the approach HCPC has taken to designing the UAF to determine how it has been ensured that a complete and accurate picture of all first line control activities have been captured and assessed. We established that the key control activities within each department were initially discussed with associate directors and that key controls were identified, captured within the UAF, and self-monitored on an ongoing basis. However, we found the controls captured within each department differ in some instances and the content and structure of the UAF differs from department to department. In organisations where the Assurance Framework is more mature, a Quality Framework has been established to define high level control principles which is then used to assess controls across departments consistently and ensure any gaps can easily be identified. However, it should be noted that this process, and implementation of the suite of iterative recommendations below may take two years to embed.** *HCPC should:* *a) Develop a Quality Framework that contains 'pillars' to create a standard way in which to assess the control environment across departments. These pillars could include Policies and Guidance, Induction and Training, Quality Checks / Peer Review, Continuous Improvement and Performance Monitoring, as examples (Year 1).* *b) For each pillar, design high level guidance setting out expectations for the expected controls to be captured within each pillar, including a good/better/best system of self-assessment to support continuous improvement (Year 1).* ***c)** 3. Ask teams to complete a self-assessment against each of the pillars, utilising the good practice guidance. Collate these responses and use them as the basis for the population of the UAF (Year 2).*		
Medium	**We discussed with managers across HCPC how the UAF operates in practice, to determine whether the approach taken is efficient and effective in ensuring the efficacy of the process and the assurances derived from the UAF. We confirmed that colleagues find the UAF valuable, particularly the regular quarterly catch ups and the process of updating the UAF supported management in considering risk. The skills, knowledge and experience of both the Quality Assurance Lead and Chief Information Security and Risk Officer in supporting management to embed controls into their processes were noted to be especially valuable. However, through our observations of the quarterly updates we noted that conversations tended to be quite reactive, and discussions were undertaken on a line-by-line basis, with the Quality Assurance Lead and Chief Information Security Risk Officer leading the discussions on each risk and control area. In organisations with more mature risk management, we would expect to see risk and UAF discussions owned by the business, with updates prepared in advance through risk discussions that are embedded within management team meetings and central colleagues taking more of a support and challenge role as part of update discussions.** *HCPC should take steps to hand the administration of the Risk Register and the UAF over to departments, undertaking monitoring to ensure that both documents become 'live' and are subject to frequent discussion within regular management fora, such as Department Management Team meetings.*		

Priority	Findings & *Recommendations*
Medium	**We examined the process for validating the efficacy of the controls in place as part of HCPC's UAF, to understand to what extend controls had been independently tested and benchmarked. Discussions with colleagues confirmed that at present the detail contained within the UAF has been gathered through their conversations with management as determine the key controls in operation within each department. No independent examination of these controls has been undertaken, over and above the general line 2 activity that is undertaken as part of their plan of work. Again, as the recommendations laid out below are predicated on implementation of recommendations 1-3, it may be that two years before HCPC is able to embed these actions.** *HCPC should, following implementation of recommendations 1-4, The Quality Assurance Team should introduce a rolling programme of reviews of team assurance maps over a three-year cycle, assessing the veracity of the self-assessment statements and providing and independent assessment of the strength of the control environment (Year 2).* *As part of the above process, collate information on best practice observed and use this to continually improve the good practice guidance and Quality Framework (Year 2).*

Priority	Findings & *Recommendations*		
Diversity		**MODERATE (DESIGN)**	**MODERATE (EFFECTIVENESS)**
Medium	**We established that managers are responsible for checking and ensuring staff members have completed the required training courses, and that "regular" reports are sent to the HoDs as a reminder to chase staff members with outstanding training. However, there is currently no enforcement procedure in place for staff members that do not complete their required training, and we were unable to confirm the specific basis on which training records are reviewed and reported upon. Additionally, the Learning and Development Manager does not have the resource in their team to chase staff members as required and ensure they complete the required training.** **Similarly, partners are also required to complete ED&I training as part of their induction. We were also unable to confirm what actions would be taken if a partner did not attend their induction to ensure they subsequently completed the ED&I training.** **During our review, four staff out of a total of 68 were found to have not completed required ED&I training during the period 09/04/2021 - 31/03/2022.** *HCPC should ensure:* *a) staff members with training outstanding are encouraged to complete their required training as soon as possible.* *b) A fixed schedule is set for reporting on training completion rates to the HoDs and the ELT.* *c) Disciplinary procedures should be formally implemented for any staff members who do not complete staff training in the required time frame.* *d) a formal sanction process is implemented if a partner does not attend their induction and complete outstanding ED&I training.*		

Priority	Findings & *Recommendations*		
Registration Forecasting		**MODERATE (DESIGN)**	**MODERATE (EFFECTIVENESS)**
High	**We reviewed the registrant data applied as 'input' information for the most recent iteration of the model (1st of September 2022) and three prior model iterations (1st of July, 1st of May and 1st of January 2022) to ensure registrant data for the prior month was correctly and accurately manually imported into the model.** **We identified that for the January iteration of the model, the input data provided was not correctly extracted and applied within the model for new international applicants (ranging between under representation of 21 and over representation 226), and for the removals of biomedical scientists (overrepresented by 77) and chiropodists & podiatrists (overrepresented by 1). Additionally, no registrant data was included in the May iteration of the model for up to the end of April 2022. We noted that the data had not been corrected on the most recent version of the model.** **The naming of input data extracted can be misleading. For example, the source of August 2022 registrant data for new international applications is labelled as "FY22 – Full Applications Total", suggesting that this is not the correct data for representing the number of new international applications. For example, within other iterations of the model, this document is labelled as "INTL APPS".** *HCPC should:* *a) Complete a reconciliation between the prior months' registrant data and historical data included within the model.* *b) Ensure input files consistently and logically labelled for each iteration of the model, to allow for consistently and help prevent error.* *c) Ensure registrant data extracted and subsequently imported into the model should be reviewed by an additional staff member to allow for a second pair of eyes oversight to help ensure model accuracy.*		
Medium	**Our review identified that the percentage of assumptions stated on the output report did not align with the assumptions used within the 'input tab' of the model. Specifically, a 90% assumption is stated in the output report for the number of future international registrations, yet a 200% assumption is applied within the model and thus it is not clear which assumption is correct and should be used to predict registrant numbers.** *HCPC should implement a method of cross-referencing is considered between the output report generated by the model and the inputs section, to prevent users from potentially being misled.*		
Medium	**Monthly meetings are held between the Chief Information Security & Risk Officer and members of other teams such as Finance and Analytics, to discuss any trends which are likely to arise which could influence the number of registrants and thus the assumptions that the model is based on. Subsequently available data will then be gathered to try and predict the impact and thus utilised to adjust the assumptions applied within the model. These meetings and the outputs from the meetings help to ensure the forecasts generated for registrant numbers are as accurate as possible and are based on real time, reasonable assumptions.**		

Priority	Findings & *Recommendations*
	Whilst no formal meeting minutes or actions are recorded, we received evidence to confirm the meetings take place. Attendance for meetings is inconsistent, with some departments not represented within meetings. Meeting attendance was advised to be consistent for the Chief Information Security & Risk Officer and the Finance and Analytics teams. *HCPC should:* *a) outline a list of required attendees for each monthly discussion to ensure a representative from each relevant team is in attendance. Additionally, if staff members do not feel the need to attend, they should notify the Chief Information Security & Risk Officer confirming they have nothing to report which could influence the parameters set within the model.* *b) Record formal actions based on the outcomes of the discussions which take place. This is to ensure that required adjustments to the model and thus the assumptions the model is based on are made timely and seem reasonable. It will also allow for any staff that could not attend the meetings to see what, if any changes have been made.*
Medium	**During a system walkthrough, we confirmed that whilst there is scope to decrease the complexity of the model the Finance department requires a breakdown of the monthly variation of applicants, registrants and removals, by profession. It is understood that a simpler version of the model previously used was not as effective at fulfilling this purpose, hence the model was expanded into its current format.** **There is scope to increase the level of integration between the outputs of the forecasting model and calculating registrant income using the number of registrants predicted. Currently, the outputs of the model must be extracted and applied into the Finance team's model, rather than included within the same spreadsheet.** **Furthermore, it was noted that currently it is not easy for the Finance team to identify the number of registrants who have discounts such as student members, when making their registrant payments and instead must manually identify the numbers. This is clearly a limitation of the model in its current form.** *HCPC should:* *a) Investigate whether it is possible to do an automated upload from the model into the financial model. If this is not possible, consider whether the model can be adapted to include what is required for the financial model with less manual intervention.* *b) A secondary check should be undertaken for all data extracted from the model that is incorporated into the financial model to verify accuracy.* *c) Consider if it is possible to incorporate and thus easily identify from the model the number of registrants on discounted registrant fees and those on full registrant fees to support the Finance team further.*

Priority	Findings & *Recommendations*
Medium	**The model is updated with new input data, including registrant data as well as assumptions, whenever a new output report is requested by the Finance team or at a minimum of a quarterly basis. Once completed, the model is then "clocked forward" and forecasted into the future. If no changes occur to the projected numbers in the model following this, the model is then investigated to ascertain the issue, and subsequently correct it.** **The primary criteria in place for investigation of any unexpected variances is 10% of the forecasted tolerances. These are for:** • **New UK registrants** • **New international applications** • **New international registrants** **Whilst the set parameter variance is included within the model, we were informed that the Chief Information Security and Risk Officer has yet to see the variance function work and is therefore unsure as to whether the function operates.** *HCPC should ensure that the Forecasting team check whether the variance analysis built into the model operates as intended.*

Priority	Findings & *Recommendations*	
Key Financial Controls Follow-Up	**MODERATE (DESIGN)**	**MODERATE (EFFECTIVENESS)**
Medium	**We reviewed the listing of finance policies and procedures which were stored on the central finance folder at the time of the audit (October 2022). There were over 116 policies and procedures within the folder. We identified via discussion with the Transactions Analyst that there is no stand-alone Procure to Pay (P2P) process, but instead this process is covered in multiple documents which are the responsibility of multiple departments.** **There is currently no policy and procedures tracker in place to document all the finance procedures, when they were last reviewed, when they are due for review and at a high-level which areas are covered as part of that policy or procedure.** **We noted that policies and procedures were not consistently up to date with current working practices, and with 116 policies and procedures, and no policy tracker in place, it is difficult for the Finance team to keep on top of when changes need to be made and when changes were last made.** **Via interviews with staff, staff relayed that they understood policies and procedures were kept in the central finance folder, but they would need to do 'some digging' to locate that folder themselves.** ***The Adding New users to WAP policy was provided to us post audit fieldwork and therefore we were unable to provide assurance on this document.*** *We recommend that HCPC:* *a) Review the composition of the 116 policies and procedures and consider whether any can be combined (e.g. P2P process).* *b) Update the Adding New Users to WAP Policy, ensuring it details how changes to individuals' access and approval thresholds are made.* *c) Create a central finance manual and policy tracker. The policy tracker should detail the date of last update (which should align to the date on the document) and detail a responsible individual for ensuring the accuracy and completeness of the policy/procedure. The tracker should detail areas covered within policies and procedures.* **d)** *Update the Finance Induction Slides to align to the above changes as well as changes from SAGE to Business Central (BC).*	
Medium	**Within section 4 of the Supplier Set-up Procedure the "Head of Financial Accounting will sign and date the report (of additions and changes), this is then included as part of the payment run pack." However, the sign-off of this task is not documented. Currently any additions and amendments of supplier bank details are assumed to be identified by the Senior Financial Accountant as part of their weekly checks before they request approval from the Head of Financial Accounting (Financial Controller).** **There is segregation of duties in place for creation and amendment of supplier bank details process. The Transactions Analyst informs the Systems Accountant of the change, they then amend the bank details, with the Senior Financial Accountant approving the payment run prior to proceeding the next payment run. The duties of the latter are to check that changes made to the system are accurate and complete as verified by information that should be provided by the supplier themselves. Once satisfied of this, the Senior Financial Accountant will download the audit log of changes made and include this in the monthly payment pack that is sent to the Financial Controller showing all approved changes. The log does not detail who has completed a review of changes and amendments to bank account details.**	

Priority	Findings & *Recommendations*
	Given these checks are insufficiently evidenced by the loading of the audit log, we checked the source documentation to confirm that bank details provided on this documentation reconciles to bank details in the SAGE system. HCPC were unable to provide source documentation for two of the four samples selected relating to the New Supplier – Vantis Technology Ltd (01/07/2022 - change made to bank details) and Crystal Services Plc (01/07/2022 - change made to bank details). *HCPC should investigate adding approvals within the finance system (for both SAGE and BC) for each addition or change to bank details, with a change of bank details being put on hold without the approval of the second individual.* *If it is not possible to require approval within the system, HCPC should look to add electronic signatures to the sign-off of each weeks' audit log, so that individuals checking these additions or changes can be held accountable for any errors not identified.*

Priority	Findings & *Recommendations*		
Cyber Security		**MODERATE (DESIGN)**	**EFFECTIVENSS (NOT RATED)**
Medium	**HCPC has defined an Infrastructure Patch Management document. Per the document, server patches are implemented as follows:** **• On-premises servers that require Microsoft service pack updates will be patched quarterly if they are internally facing and monthly if they are externally facing** **• Servers that require security updates and are externally facing must be patched within two weeks. During our assessment, we were provided with the list of missing patches as of 29 September 2022.** **Our review noted that there were 10 patches categorised as Security Updates that were missing. Of the 10 security updates, we noted the following:** **• 5 patches were released on the 13 September 2022 and fell within the 1-month period • The security update for Windows Server 2021 R2 (KB 3172729) was released on the 09 August 2016 and is missing on 4 servers within the environment** **• 2022-08 security update for Windows Server 2016 for x64 based system (KB5012170) is missing on 1 server, however this is still within the quarterly timeframe if the server is internally facing** **• Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB3185319) is missing on 1 server and was released on 13 August 2016** **• Security update for SQL Server 2016 SP2 CU17 (KB5014351) is missing on 1 server and was released on the 14 June 2022, which is outside the quarterly and monthly cycle** **• Security update for SQL Server 2016 SP2 GDR ((KB5014365) is missing on 1 server and was released on the 14 June 2022, which is outside the quarterly and monthly cycle.** *HCPC should ensure that servers be patched as per the infrastructure Patch Management policy. Where patches are not applied, it should be noted within the Risk Register and accepted at the Security Advisory Board.*		
Medium	**HCPC currently undertake quarterly vulnerability scans of their PCI-DSS Environment and use Microsoft Defender, which provides real time information of security flaws and issues present on end-user devices and servers. Currently Microsoft Defender shows that there is 71% coverage across the environment, however we noted this is because it is reporting on the decommissioned environments. Based on the evidence received, we noted the following:** **• Microsoft Defender Secure Score is 85%, with 24 active recommendations (security flaws present)** **• The flaws include applying system updates (which we have highlighted as a risk above), encryption of data in transit, applying secure configurations, enabling audit and logging, and remediation of vulnerabilities.**		

Priority	Findings & *Recommendations*
	The last PCI-DSS scan conducted in September 2022, resulted in one medium risk which has since been remediated. We further noted that the last external penetration test was conducted in February 2021. This was due to various changes within the environment which included moving systems to the cloud, decommissioning of the Demilitarised Zone (DMZ). These have required the firewall rules to be changed and as a result the penetration test has been delayed. We have noted that the change for the firewall rules to be completed was logged at the Change Advisory Board during the first week of October. The penetration test will be scheduled shortly thereafter. Furthermore, the ISO Testing Policy, which highlights the security testing requirements for HCPC was last reviewed in 2017. *HCPC, using the IT Security Risk Assessment approach which identifies how vulnerabilities are classified and prioritised within HCPC, the issues raised from Microsoft Defender should be evaluated and remediated within the required timelines. Any issues requiring further action, such as additional budget or resources should be noted within the risk register and reported to management. Regular Penetration testing should also be performed, which highlights whether the vulnerabilities present within the environment can be exploited.*
Medium	**HCPC are currently ISO 27001:2013, PCI-DSS and Cyber Essentials Plus certified. The new Head of IT and Digital Transformation joined the organisation in January 2022, prioritising moving systems and applications to the cloud and making changes to the core infrastructure. Currently there is no defined security strategy, other than maintaining the above-mentioned certifications. Every year, to set the security budget, the team discuss what the current trends are within the industry and security.** *HCPC should ensure that the security strategy is completed as soon as possible, taking input from all relevant business stakeholders, and incorporating a roadmap that aligns with the business's strategic direction, findings from audits and external rules and regulations. The security strategy should be signed off by Executive Management.*
Medium	**HCPC has deployed a Checkpoint Firewall as the perimeter firewall and Barracuda CloudGen as the web application firewall. During our review of the Web Application Firewall rules, we noted that the firewall is set as an Intrusion Detection System. This means that any malicious activity would be detected, and logs sent to the Security Incident and Event Monitoring solution for further investigation and the activity would not be blocked. The organisation has segmented their network in the form of Virtual Local Area Networks (VLANS), which reduces the risk of an attacker moving laterally and accessing other areas of the network.** *HCPC should ensure that the 'no scan' options be removed from the Barracuda CloudGen firewall rules to ensure the devices are blocking malicious activity.*
Medium	**HCPC have defined a PCI-DSS Incident Response Plan (version 1.6) that defines the steps required when responding to a security incident. The document defines what constitutes a security incident, the roles and responsibilities of the incident response team, and external contact information which includes the link to the DPA Policy for details of international breach laws and contacts details and the information of the relevant credit organisations. The document also contains high-level details for specific type of security incidents such as malware, tampering of payment terminals, unauthorised wireless access points and loss of equipment. We have noted during our review that improvements are required to the plan, including:**

Priority	Findings & *Recommendations*
	• Linkage of the plan to the IT DR Redbook **• Including details of critical IT suppliers** **• Security playbooks for other common types of attacks such as ransomware and phishing** **• Include technical recovery details for the various security incidents to aide in faster recovery of systems and information. During the review, we have noted that the incident response plan has not been regularly tested, however the team are planning a ransomware desktop simulation with the Executive team.** *HCPC should update the incident response plan per the requirements above and test the incident response plan on at least an annual basis. Testing of the plan should be matured over time, starting with desktop simulations to red/blue teaming exercises.*

Priority	Findings & *Recommendations*		
Fitness to Practise - DRAFT		**MODERATE (DESIGN)**	**MODERATE (EFFECTIVENESS)**
Medium	**We reviewed the policies, procedures and guidance (guidance) in place, such as the `fitness to practise process, information for employers and managers` policy and confirmed they provide staff with the agreed and up to date methodology for the end-to-end FtP process. The guidance references best practice themes and processes including the criteria for progressing cases. However, the guidance does not refer to the key performance indicators (KPIs) in place of completing cases within 33 weeks outside of final hearings, and 39 weeks for final hearings.** **Fitness to practise guidance is not consistently reviewed on an annual basis, for example the `FtP process, information for employees and managers` document was last updated in January 2019. There is no review timetable in place for updating FtP guidance.** **We acknowledge that as part of an ongoing review of documentation, staff are in the process of updating the FtP guidance and it is anticipated that guidance will be subject to an annual review.** *HCPC should ensure that fitness to practise policies, procedures and guidance:* *a) formally include the KPIs staff are expected to achieve for managing fitness to practise cases.* *b) Include a documented review and approval process.*		

Appendix B - Definitions

Possible Annual Opinions	
1 Substantial	There is an adequate and effective system of governance, risk management and internal control to address the risk that management's objectives are not fully achieved.
2 Moderate	There is some risk that management's objectives may not be fully achieved. Improvements are required in those areas to enhance the adequacy and / or effectiveness of governance, risk management and internal control. OR There is some risk that the system of internal control, governance and risk management will fail to meet management's objectives - some areas there are adequate and effective systems of governance, *but there are also some specific areas of significant risk*. Significant improvements are required in specific areas to improve the adequacy and / or effectiveness of governance, risk management and internal control.
3 Limited	There is considerable risk that the system of internal control, governance and risk management will fail to meet management's objectives. Significant improvements are required to improve the adequacy and / or effectiveness of governance, risk management and internal control.
4 No	The systems have failed or there is a real and substantial risk that the systems of internal control, governance and risk management will fail to meet management's objectives. Immediate action is required to improve the adequacy and / or effectiveness of governance, risk management and internal control.

Revised Ratings

We have changed the way we 'rate' our internal audit reports this year. We have moved to an opinion on the control 'design' and the control 'effectiveness', its operation in practice. The adjacent table maps the previous ratings to the new. Verbal descriptions are associated with the new levels and explained below for individual assignments and the annual opinion.

New Format (one grading for design and one for effectiveness)	Previous Format
SUBSTANTIAL	GREEN
MOERATE	GREEN / AMBER
LIMITED	AMBER
NO	AMBER / RED
NO	RED

Individual assignment recommendation ratings	
High (1) ranking:	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.
Medium (2) ranking:	There is a need to strengthen internal control or enhance business efficiency.
Low (3) ranking:	Internal control should be strengthened, but there is little risk of material loss or recommendation is of a housekeeping nature.

LEVEL OF ASSURANCE	DESIGN of internal control framework		OPERATIONAL EFFECTIVENESS of controls	
	Findings from review	Design Opinion	Findings from review	Effectiveness Opinion
SUBSTANTIAL	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
MODERATE	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
LIMITED	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
NO	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non-compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE	
HIGH	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
MEDIUM	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
LOW	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.
ADVISORY	A weakness that does not have a risk impact or consequence but has been raised to highlight areas of inefficiencies or potential best practice improvements.

Appendix C - Internal Audit Quality Assurance

Quality assurance processes and procedures	
Procedures	Our audit procedures were designed to ensure the service we deliver is of the highest standard and complies with the Public Sector Internal Audit Standards (PSIAS). We utilise specially designed internal audit software Pentana to conduct our work and all reports are subject to review by a senior manager (Stage 1) and director or partner (Stage 2). All reports are also checked for proofing errors at draft and final report stage by another staff member.
Knowledge Library	Our audit testing programmes, and good practices we find are imported into our Knowledge Library. The Knowledge Library is part of our Pentana audit workflow system and enables auditors to see examples of best practice across our client base. This enhances the quality of our audit work – understanding the features of best practice in the areas under audit and also auditing techniques applied. It also includes some standardised reporting templates.
Professional training, CPD and development	Staff are suitably professionally qualified or working towards qualification. There is a full programme of continuing professional development and training provided by BDO LLP and to specific members of the BDO LLP relating to internal audit, risk management and governance.
Quality assurance improvement programme (QAIP)	The BDO LLP has an internal audit Quality Assurance Improvement Programme (QAIP). Such a programme is a requirement of PSIAS and international internal auditing standards. It ensures that any issues identified by the quality processes are assigned actions and resolution is monitored. Specific improvements required are directed to the relevant person – generic changes to processes are recorded and tracked using the firm's internal audit quality group.
Customer satisfaction survey	We have online satisfaction surveys. These are available on a periodic 'per client' or 'per assignment' basis.
BDO client care programme	Firm-wide satisfaction survey which benchmarks our service against the firm and the industry.
Hot review	Peer review of a selection of audits to ensure each client receives the same high standards of audit work.
Cold review	The BDO LLP Risk Advisory Services Group conducts an internal 'cold review' of its internal audit working practises, reports and files annually. The review is conducted annually and was last conducted in January-February 2023. The findings feed into the QAIP.
External review	BDO LLP's internal audit work was subject to an external quality review by the IIA in 2021. BDO received the top rating of 'Generally Conforms'.

Appendix D - Limitations

We have prepared the Internal Audit Annual Report and undertaken the agreed programme of work as agreed with management and the Audit, Risk and Assurance Committee, subject to the limitations outlined below.

Limitations	
Opinion	Our opinion is based on the work undertaken as part of the Audit Strategy and Plan. The work addressed the key risk areas agreed for each individual internal audit assignments as set out in our individual assignment terms of reference. There might be weaknesses in the system of internal control that we are not aware of because they did not form part of our programme of work, were excluded from the scope of individual internal audit assignments or were not brought to our attention. As a consequence the reader should be aware that our opinion may have differed if our programme of work or scope for individual reviews was extended or other relevant matters were brought to our attention.
Internal control systems	Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.
Future periods	Our assessment of controls relating to HCPC is for the year end of the year 2022/23. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that: the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or the degree of compliance with policies and procedures may deteriorate.
Management's responsibilities	It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems. We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected, and our examinations as internal auditors should not be relied upon to disclose all fraud, defalcations or other irregularities which may exist.

FOR MORE INFORMATION:

SARAH HILLARY

BILL MITCHELL

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.