Audit Committee, 4 September 2018

Internal audit recommendations tracker

Executive summary and recommendations

At its meeting on 29 September 2011, the Committee agreed that it should receive a paper at each meeting, setting out progress on recommendations from internal audit reports.

Most of the information in the appendix is taken from the wording of the internal audit reports. The exception is the ‘update’ paragraph in the right-hand column, which provides details of progress.

Recommendations which have been implemented have been removed from this report. The original numbering of recommendations has been retained.

Decision

The Committee is requested to discuss the paper.

Background information

Please refer to individual internal audit reports for the background to recommendations.

Resource implications

None

Financial implications

None

Appendices

None

Date of paper

22 August 2018

Recommendations from internal audit reports

Recommendations summary

2018

Continuing Professional Development (considered at Audit Committee June 2018)

Recommendations summary

Priority	**Number of recommendations**
High	None
Medium	None
Low	2

	Finding and Implication	**Recommendation**	**Priority**	**Management response**	**Timescale/ Responsibility**
1	**Good Practice:** We would expect as a good practice that records are kept up to date and where possible minimising the dependency on a combination of manual and semi-automated systems, can give rise to error, omission or duplication of effort. **Finding:** Registrants who don't submit their CPD profiles by the required deadline are given a series of reminders and deadlines, which if not met are extended. Where a registrant fails to meet the deadlines set out their record on the Net Regulate system has to be 'paused' to avoid the system automatically continuing to count down and ultimately removing them from the Register. Such cases are then manually tracked on an 'Under Scrutiny' spreadsheet. Having to run a combination of manual and semi-automated systems, can give rise to error, omission or duplication of effort.	A periodic report of profiles which have remained at the 'under scrutiny' stage for extended periods should be produced and the reasons for profiles appearing on this list investigated.	Low	We acknowledge that this is a manual process but all the required data is on the spreadsheet without the need to create a separate report which will add a further manual step. We use the existing spreadsheet to identify those records which have remained at 'under scrutiny' for extended periods. Moving forward the new CPD Online Service will allow us to view reports easily with daily statistical views and advanced reporting for specific queries.	Complete

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	In the sample of 25 portfolios reviewed, one case had been marked as ‘under scrutiny’ on the Net Regulate system, and despite the required information being submitted in January 2017, and removed from the manual tracking, the details weren’t amended on Net Regulate, the registrant’s submission wasn’t acknowledged, and the profile not assessed.				
2	**Good practice:** We would expect as a good practice that assessors clearly record the decision to accept further information upon reviewing the evidence provided. This leaves a transparent audit trail leaving no ambiguity in the decision process. **Finding:** We carried out a review of 25 CPD profiles, choosing a mix of those (18) that had required further information at first assessment, those that were accepted at first assessment (7), and noted that all 25 were eventually accepted as meeting the CPD standards. Upon review of the 18 requiring additional information, we agreed with the decision reached to request additional information, albeit that in 5 cases, across two professions, the Assessors were not specific in the information that was missing.	In addition, whilst there is not a requirement for the Assessors to explain why they have accepted a CPD profile at the first assessment, management should implement a requirement that where further information has been requested from the registrant, Assessors confirm how and why any information subsequently received has rectified the original omissions. This will ensure there is a transparent audit trail leaving no ambiguity in the decision process.	Low	This is a good improvement suggestion and whilst there is no risk as we have a full audit trail of the registrant submission(s) and assessors record of assessment(s) this recommendation has been adopted and implemented with the template amended to ensure that CPD assessors provide a reason for accepting the profile.	Complete

Budgeting, Forecasting and extended Key Financial Controls Review (considered at Audit Committee June 2018)

Recommendations summary

Priority	Number of recommendations
High	None
Medium	7
Low	3

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
1	Good Practice Budgeting policies and procedures should be in place, outlining the end-to-end process, roles and responsibilities (for budget holders and reviewers) and review and sign-off procedures. There should be a clearly defined policy owner and reviewer as well as a periodic review of policies and procedures, to ensure that they remain fit for purpose. Finding We reviewed HCPC's Financial Operating Guidelines for new Budget Holders and noted that there was guidance relating to the budgeting process, key stakeholders' roles and responsibilities, and the wider end-to-end process. It was however identified that there is no requirement within the budgeting policies and procedures to submit supporting documentation in order to ascertain how the budget lines have been calculated. Refer to recommendation four, also, where it was observed for one department that supporting documentation was not provided for all expenditure included in the budget.	The Financial Operating Guidelines for New Budget Holders should include guidance regarding when supporting documentation is required to be submitted in the budget templates (i.e. where the budget line item represents 5% of the total budget value in line with HCPC expectations). Management should ensure that all policies and procedures relating to the budgeting process have clearly defined policy owners and reviewers. There should be a mandatory requirement to review relevant policies and procedures, as a minimum on an annual basis, with version control in place to ensure that budget holders are using the latest version.	Medium	Updated Guidelines for New Budget Holders to be reviewed by SMT before end of Q3. Document to be communicated out to all budget holders after approval by SMT.	Owner: Director of Finance Agreed date of implementation: From December 2018
2	Good Practice The budget setting process should encourage budget holders to manage budgets efficiently and where appropriate recognise synergies and cost savings that can be achieved, prior to initial submission to the Finance Director or equivalent. Budget holders should be challenged by Executive Management, CEO and Council for the amounts being proposed to ensure the costs are achievable and in line with expectations.	Budget holders, EMT and the CEO should consider, for example through an informal lessons learned review, whether the budgeting process can be streamlined. Executive management through consultation with	Low	The 2018-19 budgeting process took longer and more iterations needed to enable Audit Committee and Council to review earlier versions of the budget and ensure alignment with the Corporate Plan. Any changes to the budget process will go through review at the	Owner: Director of Finance Agreed date of implementation: September 2018 Audit Committee meeting

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	Finding As part of our testing, we reviewed the IT and Communications Departments' Budget Templates for 2017/2018 and identified that there were three and four iterations created and submitted, respectively. Based on our discussion with the Finance Director, a similar number of iterations also existed for other departments within HCPC. For the IT Department's budget, we noted a difference of £47k between the first submission and the approved amount by Council. Additionally, the Communications department budget differed by £76k from the initial iteration versus the amount approved by Council. The 2018/2019 budget template iterations have increased to approximately four iterations on average. Management consider that opportunities exist to reduce the number of budget template iterations created and subsequently the overall time taken to complete the budgeting process, which we understand is currently in the region of five months. We understand this was the first time that both the Audit Committee and the Council were involved in the 2018/19 budget setting process, which has been likely to increase the length of time taken to finalise the budget. We understand management are in discussions with the Audit Committee and the Council regarding the level of input required by both Committees as part of next year's budget setting process including limiting the number of iterations of the budget to a maximum of three. This should reduce the overall time taken to finalise the budget for 2019/20. Implication. A lengthy budgeting process may result in budgets taking too long to sign-off and inappropriate and inaccurate reporting (management accounts) being prepared for Executive Management.	the Audit Committee and Council, should quickly decide on the level of input required by both Committees to ensure that the length of time taken to produce next year's budget (and future budgets) is carried out within a timelier manner.		September Audit Committee meeting	
3	Good Practice Appropriate guidance and controls should be in place for changes to	Management should include a change management section within	Medium	We will review the processes for virement in the Financial Regulations and the	Owner: Director of Finance

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	the budget post Council approval. For example, additional spend on Capex. The approval process should be documented in the Financial Operating Guidelines and HCPC's Delegation of Authority (or equivalent). Finding There is no formal guidance in place detailing how changes to the budget should be managed post approval from the Council. The only relevant guidelines observed during the audit fieldwork related to the need for budget holders to achieve their budget to within +/- 5%. We also identified that there is no process in place regarding approval thresholds in instances where budget holders require additional spend due to unplanned events. Implication Without appropriate change management controls in relation to amendments to the approved budget, additional expenditure may be incurred by HCPC which is not communicated to key stakeholders such as EMT, CEO, Council and the Audit Committee.	the Financial Regulations detailing the change management process, and in particular relevant review and sign-off procedures. Approval thresholds (in percentage terms or absolute values) should be clearly documented in the Financial Operating Guidelines. In instances where budgets need to be amended, this should be formally captured and appropriately reviewed in line with the agreed thresholds.		Financial Operating Procedures that are made under the Financial Regulations. Any changes will be proposed to the November Audit Committee meeting.	Agreed date of implementation: From December 2018
4	Good Practice All amounts included with budget template spreadsheets are linked to supporting documentation to ensure that the correct amounts are being recorded, and are appropriately supported with clear evidence. Budget holders should be able to clearly justify costs through supporting documentation or through adequate justification for each budget line item. Finding Through our testing of the IT and Fitness To Practice divisions' budget templates, we identified good practice in terms of supporting documentation and audit trails being available for review. For both divisions, each line item populated in the budget template was linked	The Finance Team should ensure that, going forward, all budget template submissions and supporting evidence has been provided to validate the expenditure lines. In instances where this has not been adhered to, the Finance Team should seek further justification and evidence.	Medium	A threshold will be set out in the "Guidelines for New budget holders" and once approved; we will distribute this out to each budget holder. Finance will ensure that supporting documents are obtained for all expenditure lines above the threshold.	Owner: Head of Financial Accounting Agreed date of implementation: By December 2018

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	to supporting workings, in order to justify the costs included. However, we reviewed the Communications budget template and noted that certain amounts had been populated without a reference to supporting documentation/relevant worksheets. For example, values were manually entered into cells for the 2017/2018 budget templates totalling approximately £335k without any supporting documentation. As a result, we were unable to comment on the accuracy of budget line items against supporting information. Implication Inputting amounts into spreadsheets without reference to supporting worksheets, or other supporting information, may result in inaccurate or inappropriate budgets being produced.				
5	Good Practice Management accounts are prepared by the Finance Team on a monthly basis, and are sent to budget holders for their review and comment. The management accounts will be compared against budgets and forecasts to provide insight to budget holders regarding over/underspend. Finding We reviewed the management accounts for the IT and Communication departments and identified that although comparisons are made between year to date actual vs. year to date budget. Feedback from stakeholders interviewed indicated that whilst the above comparison has been useful, most stakeholders we spoke to wanted to have the comparison of spend for the year to date actual vs. the total budget (i.e. that was approved by Council) and this would enhance decision-making regarding potential re-allocation of budget or requests for additional spend. Implication Without appropriate analysis against the approved annual budget,	Finance should consider the feedback from other executives and discuss and agree at the next SMT what level of reporting (i.e. year to date actual vs year to date budget or any other form) is most appropriate for their needs.	Low	We agree that monthly reports should be comparing YTD actuals against YTD budget. The mid-year forecasting process will be used to redistribute resources in response to changes in circumstances, and where that occurs; those circumstances will be part of the explanation for variances between actual costs and budgeted costs. Following the EMT restructure, new budget holders are in place. We will hold meetings with the new budget holders and executive directors to discuss other management report requirements.	4/9/2018 - complete

	Finding and Implication	**Recommendation**	**Priority**	**Management response**	**Timescale/ Responsibility**
	there is a loss of accountability for the original budget.				
6	Good Practice The Finance Team should perform supplier statement reconciliations on a monthly/quarterly basis to ensure that the accounts payable balance is accurate and complete. This is typically performed through reconciling the creditor balance per HCPC's records to an external statement from the supplier; investigating any differences identified. Finding We observed on an adhoc basis that the finance team carry out an informal check to confirm supplier balances. This is carried out through an exchange of emails between the finance team and the suppliers. The evidence of the supplier confirmations are then retained on a shared finance mailbox. We observed there was no systematic filing of supplier statements and therefore the shared mailbox is just being used as a repository. The current supplier reconciliation process is not adequate, for example any differences in values arising between Sage and the suppliers' statement of account (confirmation) are not captured in the current process, and therefore there is a risk that these differences are not readily known or resolved in a timely manner. In addition, based on our sample testing of the current supplier reconciliations process, we identified one instance where the supplier statement of account was not obtained to confirm the supplier balance back to Sage. Implication Without supplier reconciliations being performed between the suppliers' statement of account and the accounts payable ledger, there is a risk that the	The Finance Team should perform supplier reconciliations on a frequent basis, to ensure that the correct amounts are recorded in Sage. Month-end close procedure documentation should be updated to ensure that there is a mandatory requirement to perform supplier statement reconciliations, which are then reviewed by the Head of Financial Accounting.	Medium	We will continue to request supplier statement and reconcile while we review Purchase Order listing and in preparation for month end Accounts Payable closing process. We will ensure better documentation (electronically) of the supplier balances we have reconciled and regular review are taking place by the financial account. During month end, Head of Financial Accounting will review the top 10 supplier to ensure supplier reconciliation took place and that they have been reviewed. We will record all approval electronically.	4/9/2018 - complete
7	Good Practice There should be a Staff Expenses Policy in place, which details	There should be clearly defined approval thresholds for different grades of line	Low	We will explore the possibility to submit staff expenses through WAP approval. We	Owner: Director of Finance

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	guidance in relation travel, subsistence, accommodation and other expense claim areas. The policy should be reviewed and approved at least annually to ensure that it remains fit for purpose. Finding Based our review of the Staff Expenses Policy in place and also reviewing the process by which staff expenses are claimed. We found the currently staff expense policy does not detail the financial limit by which line managers can approve staff expenses. It is therefore assumed in the policy all expenses, except for international travel which requires the Chief Executive's approval, can be approved by a line manager. During our testing of staff expenses we did not find any exceptions, however it is good practice for line managers based on their seniority of position, to have delegated approval limits to approve staff expenses as the first line of control. This ensures that any significant business related expenses are visible and approved by the most appropriate senior member of the management team before being sent to the finance department for secondary approval and payment. Implication Without appropriate approval thresholds in place, inappropriate staff expense claims could be approved without the appropriate visibility by senior management.	managers, within the Policy.		will update expense policy to state the threshold levels.	Agreed date of implementation: Expense policy will be submitted for review for November Audit Committee meeting.
8	Good Practice We would expect purchase orders to be raise in timely manner, and not raised retrospectively. Furthermore, we would expect approved purchase orders to be closed once the invoice(s) has been received and processed. Finding Through our discussions with the Finance Team, and subsequent	POs should be raised in a timely manner, but more importantly the budget holder/approver should not approve any intent to purchase goods/services without a valid PO. This will prevent the majority of retrospective POs being raised.	Medium	Meetings to be held with budget holders and performance of regular review to start before end of Q2 We will address inappropriate use of retrospective POs through informal communication with	Owner: Head of Financial Accounting Agreed date of implementation: September 2018

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	and fieldwork, we identified that there are no formal processes or controls in place for tracking employees who consistently raise POs in an untimely fashion or through the use of old POs, in order to identify and provide training for the individuals involved. Whilst our sample testing did not find any retrospective POs, management are aware of late POs being raised. This further suggests that the current process for raising purchase orders cannot be relied on as staff could raise purchase orders once invoices are sent by relevant suppliers. We understand since our fieldwork that Management have taken action to communicate with staff to prohibit the use of existing purchase orders. Implication Without appropriate controls for identifying staff who consistently create POs in an untimely fashion, HCPC may be committing to expenditure, without appropriate purchase orders being raised.	Management should also track retrospective POs and report these at an appropriate committee, for example SMT for oversight.		the budget holders concerned and their line managers if appropriate. Reporting to a Committee is not required.	
9	Good Practice Changes to supplier master data should be reviewed on a regular basis, for example monthly, in order to validate the completeness and accuracy of such changes. Where supplier bank details are required to be changed/amended. We would expect to see: • segregation of duties internally within HCPC for approval of any changes to bank details • HCPC to carry out a check with the company (typically fraud occurs through trusted and known individuals) • management to review and approve (i.e. monthly) changes supplier master data. Finding	Given that the organisation has a system in place that allows it to capture changes to supplier information, we would strongly recommend that the system is used to capture the approval (through the new Sage plug-in or equivalent) of changes by an appropriate and authorised individual(s). Management should introduce a formal control, which requires a periodic (monthly) review and approval of changes to supplier master data,	Medium	We have obtained the license string for this function; this will be apply to the system in June 18. We will include a new step in the weekly payment run, to ensure a report has been run to show that all changes made to the supplier database are approved. We will investigate this with Sage and investigate any risks associated or unintended consequences associated with carrying out this action.	4/9/2018 - Complete

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	Based on our audit work, we carried out checks to understand the whether changes to supplier master data including bank details are reviewed and approved in a timely manner. We found through our fieldwork and discussions that the HCPC have the ability to run an audit log report from Sage, which picks up changes to supplier master data (including bank details, business address, and contact details). However, we found that the report has not been run on a regular basis, if at all. We were provided with the audit log during our field work, and noted from our review of the report, that the ‘approved on’ date fields were blank, and we were therefore unable to ascertain whether approvals were provided for relevant amendments through the right process/system. Discussions with the Head of Finance identified that HCPC are working with Sage to create a plug-in, where appropriate approval can be obtained, prior to making any changes to the supplier master data. Furthermore, based on our fieldwork, we were able to validate that appropriate segregation of duty controls are in place as the Transactions Team and IT super-users are the only individuals who have access in Sage 200, to make changes to supplier master data Through our discussions with the Head of Finance, we noted that IT super-users do not have Sage installed on their computers and therefore, are currently unable to make changes to supplier master data. Finally, we reviewed a sample of spot checks performed regarding changes to supplier master data through validating the bank account details on the BACs run to the supplier invoice however, this is currently being performed on an ad-hoc basis by the Head of Finance. Implication There is a risk that inappropriate or fraudulent changes could be made to supplier master data, such as bank details, and this would not be identified as the change report is not reviewed, and amendments are not agreed to supporting documentation and approved prior to changes being made.	including agreement to supporting documentation, and confirmation through discussion with the supplier. Management should evaluate whether Sage is able to provide the relevant reports/data extracts to be able to compare supplier and employee bank account details; for example through exporting data into Microsoft Excel and running a ‘V look up’ query.			

	Finding and Implication	**Recommendation**	**Priority**	**Management response**	**Timescale/ Responsibility**
10	Good Practice There should be guidance available to the Finance Team detailing how journals should be prepared, reviewed and subsequently posted into the accounting system, Sage. Finding During our discussions with the Finance Team, supported by testing performed, it was identified that there is currently no documented procedural guidance detailing how journals should be prepared and reviewed, prior to being posted. Based on our discussions with the Finance Director, journals are reviewed by the Head of Finance on a monthly basis, however, this review takes place after journals have been posted, as opposed to before posting in the Sage finance system in line with good practice. Implication Without appropriate procedures in place for journal postings, audit trail requirements and review processes, incorrect or inappropriate amounts may be posted to the general ledger. This could also lead to the need for journals to be corrected, increasing the administrative requirements of the Finance Team.	Management should create a formalised journal posting procedure which includes, but is not limited to, the following: • Journal preparation procedures • Journal review processes • The process for recording the journal within the Sage finance system.	Medium	We will create guidance to show the journal posting procedure. We have ensured that segregation of duty exists between reviewer and submitter of journals. All journals are showing in the transaction listing and reviewed by budget holder as part of month-end review process. To avoid creating a bottleneck and delay month end processes, journals are reviewed after they are posted, but before we finalise the month end account. The current financial system does not support approval routes for journals. We will have to keep the current process until a new system is in place.	Owner: Head of Financial Accounting Agreed date of implementation: September 2018

Cyber Security Review (considered at Audit Committee March 2018)

Recommendations summary

Priority	**Number of recommendations**
High	None
Medium	3
Low	5

	Finding and Implication	**Recommendation**	**Priority**	**Management response**	**Timescale/ Responsibility**
1	Good Practice Access management is a key area within an IT security framework, as it should ensure that data is only accessible to authorised and necessary individuals. It is good practice to implement processes to ensure that all access requests (and changes to existing access rights) are reviewed and approved before being granted, and that access is removed when no longer necessary. In addition, periodically reviewing users' access rights ensures that access remains appropriate and commensurate with job responsibilities. Finding We noted that HCPC management has begun to request that department heads revalidate appropriateness of access for users who have access to their respective departments' share drive on a monthly basis. However, not all department heads were revalidating this access as requested. Additionally, there is no documented process in place that provides a path to escalate this non response and ensure that access is ultimately reviewed on the frequency defined by management. Access to organisation-wide assets such as the network is key to ensuring that HCPC can demonstrate that it is appropriately implementing security controls to protect personal data that is held by HCPC.	**R1:** Management should develop policies and procedures to formalise the monthly user access review process, including an escalation process if non response persists from department heads. Additionally, management should coordinate with department heads and line managers throughout the organisation to identify opportunities to expand this user access review to include application level access that may be provisioned at the department level such as HCPC's core financial systems, which are provisioned by the finance department.	Medium	Robust controls for the starters and leavers process enforce access controls to the network infrastructure. The current procedure for managing user access prevents a user from accumulating access rights by enforcing rights that are specific to a single team and role. Secondary access controls are maintained within business applications and are maintained by each specialist business teams. A policy and procedure will be developed to clarify the user access revalidation process including the escalation procedure for this secondary control. . The IT team will work with the Business Process Improvement team to support the coordination of the review of access revalidation for each affected business application by the business owners.	4/9/2018 – complete

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	Implication Responsibilities for access management span across multiple departments (IT, HR, line managers, facilities), requiring coordination. This leads to a greater risk of a user's access not being appropriately removed when necessary. There is a risk that a user with excessive or inappropriate access may retain access to a shared drive for longer than necessary if department heads do not respond to the monthly user access review requests.				
2	Good Practice As significant efficiencies and expertise can be gained through the use of third party-managed services, management must ensure that the appropriate protections and requirements are in place to ensure that management has sufficient oversight into the security of the third party service, and an understanding of how the third party may impact the cyber security posture of the organisation. Finding It was noted that HCPC utilises a third party service provider, Rackspace, to provide hosting services primarily for HCPC's external-facing website. Rackspace provides monthly reports disclosing the percentage of time in the past month the service was running (uptime) and a listing of the outstanding service and security issues that require solutions to HCPC. These reports, however, do not detail the age of open tickets, including those that are labelled as security-related. Additionally, there are no defined expectations (for example a Service Level Agreement) between HCPC and Rackspace for their responsiveness to security-related tickets. Implication A lack of reporting of security ticket aging may result in a	Management should consult with Rackspace to determine if the aging of tickets can be reported to HCPC management on a monthly basis in conjunction with the monthly status report. Management should request that service levels are agreed, in relation to how responsive Rackspace must be in addressing security-related incidents.	Medium	Rackspace are currently investigating the feasibility of creating a specific report detailing the aging of security related events; improved reporting will be implemented if feasible. Security related incidents are currently assigned to a standard SLA as Emergency, Urgent or Standard with response times from 15 minutes to 4 hours depending upon the nature of the incident. We will work with Rackspace to clarify the rules that determine which service level is applied to a particular incident type.	4/9/2018 - complete

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	security-related ticket going unaddressed for an inappropriate length of time without the awareness of HCPC management. Such open tickets would have an impact in HCPC's cyber security posture.				
3	Good Practice Removable media (such as CDs and USB drives) are used in organisations to fulfil operational purposes, but can pose a risk to security. For example, removable devices can introduce malicious viruses to an organisation's network, or be used to take sensitive data outside of the organisation. Finding HCPC has implemented an automated solution to restrict the usage of removable media to a "whitelisted" set of approved devices that are required to be encrypted, and continuously scanned for malware. However, IT management does not retain documentation related to the (1) owner and (2) justification related to each whitelisted device. Implication Without a record of the personnel responsible for each approved removable device and its associated justification, management is unable to perform reviews of approved devices to ensure that the devices continue to be required, or who is responsible for devices if it is detected that one may have been used to leak sensitive information outside of HCPC's control. Such documentation is critical to allowing management to continuously monitor the appropriate usage of removable media throughout the organisation.	Management should revise the provisioning process for removable devices to require that all users requesting removable storage complete documentation noting who is responsible for the safekeeping and proper use of the device, and the justification for the device. Management should consider removing all devices that are currently whitelisted using the Symantec Endpoint Protection solution in place. This action would force users to re-request permission for their removable device to access the network and complete the revised process where the devices' owner and justification is retained.	Medium	A new policy will be created to clarify the management of removable media devices including the requirement for a business justification. All existing whitelisted storage devices will be removed and new removable media issued through the new policy.	4/9/2018 - complete
4	Good Practice The implementation of automated IT security monitoring tools	Management should design and document standardised process to continuously	Low	The HCPC currently use advanced threat detection tools to monitor and alert against suspicious	Complete – 4/9/2018

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	can greatly improve an IT department's ability to have a more holistic view of the organisation's security posture. Appropriate processes should be developed by the organisation to manage these tools and the alerts and information that is generated by them so that the full value of their use can be realised. Finding HCPC management has recently implemented and started to use the Microsoft Advanced Analytics (ATA) package as well as CimTrack to monitor user activity and monitor the integrity of data on perimeter devices, respectively. However, management has not yet developed the processes to manage and escalate relevant alerts to ensure that potential security incidents and anomalies are continuously identified and addressed. Implication Implementing tools such as Microsoft ATA and CimTrak is an effective first step, and developing processes to manage these tools will assist HCPC in leveraging these tools to a greater extent. With the lack of defined supporting processes, HCPC is at risk of not having a uniform understanding of how the tools are to be used and integrated into day-to-day operations.	monitor alerts and insights that are developed from IT security monitoring tools. Management should ensure that these processes align with the organisation's ways of working, and that the processes allow management to leverage and disseminate insight gained from these tools to relevant teams and personnel.		activity. The process for managing intelligence gathered by these tools will be formalised and documented to standardise the threat response from the IT team.	
5	Good Practice The use of secure and encrypted communication across the internet helps ensure that an organisation's communications cannot be intercepted and read by malicious actors. Finding HCPC utilises a bulk email messaging service to send non confidential emails to Registrants. This bulk email service first sends the messages to a service that will scan the messages	Management should consider utilising alternative email protocols (such as SMTP-Secure) and services that would encrypt email communication, if the risk associated with the current state is determined to be high enough to merit action. Management should	Low	This delivery mechanism will be replaced with the implementation of the second phase of the Registration Transformation project. It should be noted that the secure delivery of email is also determined by intermediary internet service providers and by the method which the recipient receives their email, for which the HCPC has no control. However, we will investigate with	Complete – 4/9/2018

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	for any potential viruses, encrypt them, and then send them to Registrants. This messaging service, however, does not encrypt messages when they are first sent to the anti-virus scanning service. The messaging technology that is used during this first step is called Simple Mail Transfer Protocol (SMTP). Confidential emails are sent through separate email services which support encryption. Implication As emails are not encrypted as they are transmitted to the anti-virus provider, there is a risk that these bulk messages sent from HCPC could be intercepted and read by an unauthorised individual.	consider revising firewall configurations appropriately if an alternative protocol is identified.		the HCPC email service provider whether an alternative secure email protocol could be used to deliver email securely to their bulk mail service for the period before its replacement.	
6	Good Practice Ensuring that IT assets throughout the network are equipped with the latest patches for operating systems and applications helps strengthen an organisation's cyber security posture by ensuring that programs being used are not susceptible to known vulnerabilities. Most patches are released on a periodic cycle, meaning that an organisation can plan in advance to test and apply them when they become available. Testing patches is important in ensuring that the fix that was released by the vendor does not impact the functionality of services in an organisation’s unique environment However, from time to time vendors release ‘emergency patches’, these tend to address critical security flaws, are released with little advance warning, and need to be applied in a short time frame. Having a process in place for addressing emergency patching helps ensure that devices are patched in a timely manner that is commensurate with risk. Organisations will sometimes decide to implement these patches into production without testing them, which adds more risk, as the	Management should consider revising the emergency patching process to require that the SAB is consulted and provides final approval for emergency patches via email and during a scheduled meeting.	Low	The terms of reference for the Security Advisory Board have been amended to require emergency patches to be authorised through the board.	Complete – 4/9/2018

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	patch could force a machine or part of the network to stop working due to the organisation's unique IT environment. Finding A process is in place to approve emergency patches in the HCPC IT environment without being formally tested if approved by the IT Director. It was noted, however, that the Security Advisory Board (SAB) (created in October 2017) may be a more appropriate forum to approve emergency patches. While it is common for organisations to implement untested patches, there is risk involved; based on the documented responsibilities of the SAB, it appears that it would be within their responsibilities to provide this final approval. Implication There is a risk that the decision to implement critical patches into the production environment is not fully considered if the SAB is not involved in this process. This may result in a lack of proper and defined oversight over the security of the IT environment.				
7	Good Practice Physical environment controls are typically necessary when installing IT infrastructure equipment to ensure that availability of the network is not impacted from water damage, overheating, and fire. IT server and equipment stacks should always be on elevated flooring and in a room that is not susceptible to water damage. Finding HCPC's key IT services are hosted on servers which are housed in a server room located in the Kennington office. The equipment stacks, which include network firewalls, are not on elevated flooring. The server room is located near the toilets,	Management should assess alternative sites throughout the Kennington office to move the server room and conduct an analysis of alternatives sites within current premises to ensure that the risk of water damage and flooding are kept at an acceptable level. Alternatively, management should install raised flooring for the server room to	Low	As part of the 186 Kennington Park road building renovation the toilets adjacent to the server room and on the second floor will be removed which will mitigate this risk. However, as part of the budget setting and work planning process for 2018-2019 a project to move the server room will be accessed as part of a larger service improvement plan.	Complete – 4/9/2018

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	increasing the risk of water damage. We did note however that the ground floor was elevated from the road, and thus was protected from low-level flooding from outside the building. Implication There is a risk that in the unexpected event of building water damage or plumbing issues, the network's services and firewalls would not be appropriately protected. There are increased risks to the server being housed next to a toilet, increasing the likelihood of water damage. Server rooms in basements also pose a risk to water damage, as water has a higher chance of leaking from above floors, and basements are more susceptible to flooding damage.	reduce the risk of water damage.			
8	Good Practice Policy and procedural documentation are key to ensuring that an organisation's institutional knowledge is retained and effectively communicated throughout the organisation. Policies and procedures regarding the management of network firewalls helps ensure the continuous and uniform upkeep of network firewalls. Finding It was noted during our review that the firewalls at Rackspace are owned and managed by Rackspace. However, this contradicts the HCPC's 'Perimeter Firewall Policy' which states that all the perimeter firewalls are managed by HCPC IT engineers. Risk Unclear documented roles and responsibilities with HCPC and third party providers may result in a lack of uniform management and understanding of how the HCPC manages firewalls. This could have an impact when sharing, delegating,	Management should update The Perimeter Firewall Policy to correctly reflect ownership and management of all firewalls.	Low	The configuration of the firewalls managed by Rackspace are specified by the HCPC Infrastructure Engineers and a rigorous authorisation process is in place to control changes. The current Perimeter Firewall Policy will be updated to reflect that although HCPC specify the firewall rules the firewalls are maintained through a managed service by Rackspace.	Complete – 4/9/2018

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
	or passing on IT-security related responsibilities and understanding to new personnel.				

2017

Review of Recruitment and Retention (considered at Audit Committee March 2017)

Recommendations summary

Priority	**Number of recommendations**
High	None
Medium	None
Low	3

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
3	Existing recruitment procedural guidance is contained in a number of individual documents, these include: • Interview assessment guidance • Stages of the interview guidance • Process flowchart for recruitment A number of these documents were last reviewed/updated in December 2015. Training in the guidance was also last provided in December 2015. The recruiting managers that we interviewed during the review all stated that they would benefit from further training in the recruitment process. Failure to have procedural guidance in a single location, complemented with recent training, may lead to recruiting managers not comprehensively following the agreed process. This may lead to external challenge over the process.	The HR Business Partner should ensure that all recruitment procedural guidance is reviewed, up to date and maintained in a single place for ease of access. Recruitment training should also be offered to all existing and new Recruitment Managers and recruitment panel members.	Low	Recruitment Guidance will be reviewed and training delivered as part of our on-going 'HR Essentials' programme by March 2018	Director of Human Resources **Update** 04/09/2018 - Complete **Previous updates** 21/11/2017 – This work is due to be completed by march 2018

2016

Review of Whistleblowing arrangements (report dated August 2016 – considered at Audit Committee 6 September 2016)

Recommendations summary

Priority	Number of recommendations
High	None
Medium	2
Low	1

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
1	Since becoming a prescribed person in October 2014, the Council at its meeting in March 2015 considered the Francis Report on Freedom to Speak Up and made a number of commitments to be completed within agreed timescales. One of these was to continue work in 2015/16 on developing an organisation-wide process for identifying, recording and handling protected disclosures made to the HCPC as a prescribed person under PIDA. The Director of Policy and Standards informed us that management had recently published more detailed information on its website about making such disclosures (as part of an existing section for registrants on reporting and escalating concerns). An internal policy setting out what is means to be a prescribed person and what procedures need to be followed had not yet been produced, but is planned for autumn 2016. The Council should use the launch of this policy to promote the role of the HCPC as a prescribed person to managers and staff and to brief and/or train as appropriate those who might receive such disclosures. There may not be clarity within the HCPC in how to deal with disclosures to it as a prescribed person without a policy.	The Council should ensure that a Prescribed Persons Policy is developed, approved and introduced within an agreed timescale and monitored. All employees, partners and Council and committee members should be made aware of the new policy so that the HCPC's role as a prescribed person is clear and understood.	Medium	Recent discussion with the Solicitor to Council has confirmed that we are compliant with the legal expectations placed on us as a prescribed person. We agree, however, that an internal policy which can be used to raise awareness across the organisation of our role as a prescribed person would be very helpful. A policy will be produced and agreed by the Executive Management Team in 2016, with progress reported in the Policy and Standards Directorate report to Council.	Director of Policy and Standards **Update** 04/09/2018 – Complete. A policy was agreed by SMT 7 August 2018. **Previous updates** 21/11/2017 – No change 14/06/2017 – Under development. This will now be informed by a meeting with other regulators to take place in July 2017

	Finding and Implication	Recommendation	Priority	Management response	Timescale/ Responsibility
					15/03/2017 - This work is now expected to be considered by the EMT in March 2017 22/11/2016 – This is underdevelopment and is due to be considered by the Executive Management Team in January 2017.

2015

Review of five year plan model functionality and controls review (report dated November 2015 – considered at Audit Committee 26 November 2015)

This report was not presented in traditional observation/recommendation/management response format. Observations that did not have an associated recommendation and recommendations that have been implemented have not been reproduced. The following recommendations are still open.

	Recommendation	Priority	Management response	Timescale/ Responsibility
Fitness to practise section of the model				
	We did not identify any major issues with inserting new data to reforecast the 5 year plan based on updated actuals. We do however recommend inserting a model version tracker as a way of assessing performance against the budget and long term forecasts. We note that it is not currently possible to change the forecast dates for FtP costs independently to other calculations and understand this functionality may be helpful. One approach would be to insert a flag to limit	Low	Noted, though to reforecast, the start and end date of the budget actuals would need to change, which impacts on registrant numbers calculated elsewhere.	Finance Director / Director of Fitness to Practise **Update** **Previous updates**

	Recommendation	Priority	Management response	Timescale/ Responsibility
	changes to forecast and actual periods to only the FTP sections of the model. However when implementing this we would recommend that this is clearly reported to users so they are aware of assumptions being used			21/11/2017 – No change 05/09/2017 – Work on this was suspended when one of the key participants went on maternity leave and has not been taken further as other projects are currently higher priority. 14/06/2017 – Work still underway 15/03/2017 – The work has started but is still underway 22/11/2016 – This work has slipped and is now starting in November with the aim of completing by the end of the financial year. 06/09/2016 – Finance and FTP are working together with the aim of integrating the FTP module of the 5 year plan with FTP's workforce planning and management information systems. These recommendations will be considered as part of that work, due to complete by November 2016.
	We have observed that the model can cannot currently be used for sensitivity analysis or as a resource /workflow planning tool. In the models current state the addition of monthly updates to enable resource planning and effective reforecasting would require a periodic freeze of the registrant assumptions. This would also drive the need for a reconciliation/ logic check between the frozen and updated registrant values. Implementing this would require an update of the model with sufficient testing to ensure a robust procedure for updating inputs and reconciling frozen values.	Low	Noted and agreed. We'd want to do this to assist with future budget planning and resource management, especially to monitor the impact of planned changes in FTP processes and structures.	