Audit Committee 13 March 2013

Internal audit – Review of recommendations

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

1 March 2013

Recommendations from internal audit reports

Information Security/Data protection (report dated September 2011 – considered at Audit Committee 29 September 2011)

Assurance on effectiveness of internal controls: Substantial Assurance

Recommendations summary

Priority	Number of recommendations
Fundamental	None
Significant	None
Housekeeping	9

Risk 1: Electronic data is removed inappropriately by an employee (Data Security – Risk No 17.1)

	Observation/Risk	Recommendation	Priority	Management response	Timescale/responsibility
1	*Observation:* Staff are asked to sign up to the Information Technology Policy under section 5h of the Employee Handbook. This policy details the responsibilities of the staff and the use of devices such as laptops and PDA's and use of email, telephone calls etc. Whilst it mentions that information held on USB drives is the property of HCPC, it does not mention HCPC's specific policy in respect of these tools. For example, the responsibilities of Staff using USB drives, that only encrypted	As planned, HCPC should review and update the Information Technology Policy held within the Employee Handbook to ensure it provides more detail on the use of USB data drives.	Housekeeping	A review of the IT Policy is scheduled for 2012-13 financial year. These updates will reflect changes in technology that are rolled out to the organisation over the next few months	2012-13 Financial year Director of HR /Director of IT **Update:** The USB controls are in operation in the Registration, FTP, Partners, Secretariat and Policy departments. The software is now being deployed as part of the Windows 7 PC upgrade to the whole of the

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
2013-03-01	a	AUD	PPR	Executive summary review of recommendations Audit Committee 13 March 2013	Final DD: None	Public RD: None

2

drives can be used, what USBs should be used for and the security of these. We were informed that the Policy is currently being reviewed and should be in place from September 2011. *Risk:* Staff are not fully aware of their responsibilities in respect of the use of USB data drives.							organisation and is expected to conclude early in the new financial year. The IT Policy has been through a legal review and will be presented on March 26 to EMT; it will then be presented to the Finance and Resources committee at the next meeting in either April or June 2013.

Follow up of previous recommendations (report dated September 2011 – considered at Audit Committee 29 September 2011)

	Observation/ Risk	Original category	Original management response and update response as of September 2011	Implementation date and manager responsible	Status	Comments/ implication	New recommendation
1	Management should complete the steps necessary by September 2011 towards removing the option for individuals to	Medium	Agreed. The system changes are required for both PRS and Sage to ensure that the full benefits are realised and to ensure cross product	Sept 11 Director of Finance	The agreed date for implement ation of the recommen dation has not yet	The implementation date for this recommendation had not yet been reached at the time of carrying out this audit. However, the upgrades required	Management should complete the steps necessary towards removing the option for individuals to follow manual procedures when raising supplier purchase

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
2013-03-01	a	AUD	PPR	Executive summary review of recommendations Audit Committee 13 March 2013	Final DD: None	Public RD: None

3

					been reached	have been delayed until next year. HCPC are currently undergoing several projects involving systems upgrades including major projects relating to Case Management and Fitness to Practice in anticipation of taking over responsibilities relating to GSCC and these have been prioritised.	orders. (Significant) **Updated management comment:** The procurement, requisitions and purchases procedures will be reconsidered to include a revised tendering policy and proposals for the supplier database A procurement and tendering update will be presented to the Finance and Resources Committee on 19 March 2013. Recruitment is underway for a Procurement Manager.
follow manual procedures when raising supplier purchase orders.		compatibility. This should be implemented in the FY 2011/12, subject to budget approval.					

Core Financial Systems – Payroll (report dated September 2011 – considered at Audit Committee 29 September 2011)

Assurance on effectiveness of internal controls: Substantial Assurance

Recommendations summary

Priority	**Number of recommendations**
Fundamental	None
Significant	None

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
2013-03-01	a	AUD	PPR	Executive summary review of recommendations Audit Committee 13 March 2013	Final DD: None	Public RD: None

Housekeeping   3

Risk 3: Financial losses arising from fraud or error, inefficient processing or inappropriate activity (such as ghost employees, payment of staff who no longer work at the Council, authorised payments, etc)

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
2	*Observation:* Finance receive an HR Pack on a monthly basis which includes the HR Summary spreadsheet and relevant supporting documentation detailing starters; leavers; contractual variations; acting-up allowances; changes to address etc. Whilst our review confirmed that this information was received by Finance, in a timely manner and before the deadline of the 15th of the month, as there is currently no direct interface between the HR Systems and Sage, the information has to be entered again on to Sage. It is noted that a review of the HR system is planned to be undertaken. *Risk:* Holding two databases with staff details and duplication of data entry are unlikely to be an efficient use of resources.	As part of the planned review of the HR system, consideration should be given to a more effective interface between the HR and Payroll systems to avoid duplication in entry of data.	Housekeeping	Project proposal to review HR & partners information systems, including link to payroll to be submitted to Executive team in November 2011. If agreed will form part of 2012/13 project plan.	Director of Finance/ HR Director. Timescales pending outcome of Executive Team meeting November 2011 **Update**: HR & Partners Systems & Process Review Phase 1 is due to take place between 01/04/13 - 31/12/13

	Errors are more likely to arise where data is re-keyed.				

ICT Security (report dated November 2012 – considered at Audit Committee 28 November 2012)

Assurance on effectiveness of internal controls: Substantial Assurance

Recommendations summary

Priority	**Number of recommendations**
Fundamental	None
Significant	None
Housekeeping	3

Risk 1: Electronic data is removed inappropriately by an employee (Data Security – Risk No 17.1)

Risk 2: Malicious damage from unauthorised access (Information Technology – Risk No 5.5)

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
1	*Observation:* An Information Technology Policy is documented as part of the staff handbook. The policy covers a number of standard including acceptable use, the ownership of systems, security over passwords and the monitoring mechanisms in place. Users are required to sign-up to this policy on joining the organisation as part of the awareness of the wider	As planned, HCPC should review and update the Information Technology Policy held within the Employee Handbook to ensure it provides more detail on the	Housekeeping	The IT policy is being reviewed as part of the 2012-13 IT Work Plan.	Director of IT **Update:** The USB controls are in operation in the Registration, FTP, Partners, Secretariat and Policy departments. The software is now being deployed as part of

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
2013-03-01	a	AUD	PPR	Executive summary review of recommendations Audit Committee 13 March 2013	Final DD: None	Public RD: None

6

	handbook. However there are some matters which require review and the policy is currently in the process of being updated. The Director of ICT has liaised with a number of similar organisations in the sector to obtain their IT Security policies to benchmark against. *Risk:* Policy in place does not reflect current practice, intention or controls.	use of USB data drives and reflects current technologies and policy on the use of IT.			the Windows 7 PC upgrade to the whole of the organisation and is expected to conclude early in the new financial year. The IT Policy has been through a legal review and will be presented on March 26 to EMT; it will then be presented to the Finance and Resources committee at the next meeting in either April or June 2013.
2	*Observation:* Penetration testing of both Infrastructure and Applications is carried out by a third party contractor, NCC Group, on a quarterly basis but from an external only perspective. The recent reports indicate overall good security practices are implemented across the majority of the external network infrastructure and the latest report dated July 2012 highlights no high or medium level vulnerabilities in either the application or supporting infrastructure. However, as yet no penetration testing	HCPC should consider undertaking penetration testing from an internal perspective to provide a full assessment of the environment and confirm all internal controls are operating as expected.	Housekeeping	Penetration testing from an internal perspective will be considered as part of the 2013-14 IT Work Plan.	Director of IT Update: Penetration testing from an internal perspective is being considered as part of the 2013-14 IT workplan due to be presented to the Finance and Resources Committee on 19 March 2013

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
2013-03-01	a	AUD	PPR	Executive summary review of recommendations Audit Committee 13 March 2013	Final DD: None	Public RD: None

7

	has been conducted from an internal perspective inside the business. Given the broadly clean bill of health from the externally facing infrastructure, testing of the internal infrastructure and risks internally would be the next logical step in ensuring the security of the network. *Risk:* Internal penetration risks exist which put the control environment at risk.				
3	*Observation:* There has been no exchange of data between HCPC and the system supplier for 'NetRegulate', Digital Steps Limited (DSL) that can be remembered by IT Staff. Controls and expectations are outlined in the contracted arrangements between the two parties and these were reinforced by letter in 2010. A secure facility, known as 'Jump and Dump' has also been established to provide secure access for the suppler and to prevent the supplier removing data without the express permission of HCPC. However, despite both of these controls there is no formal mechanism to confirm destruction of data should it be required. Risk: Confidential data exists outside the control of HCPC and at risk of	In the event that live data is exchanged in the future then HCPC should request written confirmation from DSL that the data has been destroyed once no longer required.	Housekeeping	DSL currently only hold HCPC data that has been anonymised. In future where projects require data in its original form, i.e. not anonymised, then we will request written confirmation that data has been deleted following the closure of the project it was intended for.	**Update:** written confirmation that data has been deleted will be sought in future when projects close.

	unauthorised usage or access.				

Income Collection & Debtors (report dated September 2012 – considered at Audit Committee 28 November 2012)

Assurance on effectiveness of internal controls: Substantial Assurance

Recommendations summary

Priority	Number of recommendations
Fundamental	None
Significant	None
Housekeeping	3

Risk 1: Inability to collect from debtors (Finance – Risk No 15.6)

	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
1	*Observation:* Currently, all payments received by cheque, postal order and cash are initially processed on NetRegulate by Registration Advisors and then all information is transferred to Finance – Transactions team for checking and processing the following day. The same cheque/postal order is reviewed and checked twice (once in Registrations when it is input to NetRegulate, and once in Finance as part of the daily banking). It is not clear that the checking of each cheque/postal	Consideration should be given to reviewing the processes for checking and banking of income received by cheque, postal order and credit /debit card to ensure that the most efficient process is in	Housekeeping	We agree that the way this process is currently handled is not the most efficient and consideration will be given to ways of eliminating the duplication of tasks.	October 2012 Director of Finance/Head of Registration Improvements to this system are now a part of the HCPC project prioritisation plan. Timescale: Net Regulate changes

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
2013-03-01	a	AUD	PPR	Executive summary review of recommendations Audit Committee 13 March 2013	Final DD: None	Public RD: None

9

	order in Finance, which may take a considerable amount of time, adds much value in addition to the original check performed by Registrations. The checking of cheques and postal orders is not the main role of Registration Advisors who primarily deal with processing application forms and advising registrants and applicants on matters relating to their registration. Therefore a 'cashier' role specifically dealing with cheques, postal orders and credit/debit card payments and not dealing with other parts of the Registration process may be more efficient and less likely to produce errors. Such a role would reduce or remove the need for additional checks in Finance – Transactions and would also speed up the processing, such that transactions processed on NetRegulate by Registrations would not have to wait until the following day to be checked and processed in Finance – Transactions, but could be banked the same day – thereby reducing problems around cut-off at the end of each month. *Risk:* Duplication of effort resulting in inefficient use of resources.	place. For example, the current checking performed by Registrations and Finance and the potential for a 'Cashier' role.			2012-13 01/01/13 - 31/03/13
	Issue: Timing difference at	Currently, this has	Housekeeping	NetRegulate process	Head of

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
2013-03-01	a	AUD	PPR	Executive summary review of recommendations Audit Committee 13 March 2013	Final DD: None	Public RD: None

10

	month end date – On the last working day of the month, transactions are posted by the Registration team on NetRegulate which are not processed by the Finance team until the following day. *Recommendation:* Finance team to work with Registration team to ensure that items posted on last working day of month in NetRegulate are also processed on the same day	been resolved by members of the Finance – Transactions team staying late at month-end to ensure transactions are processed the same day.		changes are being developed by DSL to enable us to produce a monthly report to show exactly what is being processed at month end.	Financial Accounting These changes are now a part of the HCPC project prioritisation plan. Timescale: Net Regulate changes 2012-13 01/01/13 - 31/03/13
	Issue: Correction Adjustments - where a registrant's record is updated using a correction adjustment, the treatment of the way the record is accounted for differs depending on the reason. A main cause of difference has been identified as re-admission reverse charges which are not shown on the transfer report. *Recommendation:* As a temporary work around going forward, Finance team to obtain a DBA Visualizer (based on an SQL query) report from NetRegulate at month end and manually adjust any mis-postings in Sage. A NetRegulate change request will be created to amend NetRegulate to automatically take account of these	As planned, a solution involving updating the NetRegulate system to automatically take account of these transactions should be implemented.		As part of the automated Readmission project, reversal readmission charges will no longer be posted. This change will remove this issue.	December 2012 Project team Update: The automated readmissions project is currently due for completion on 31/01/13

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
2013-03-01	a	AUD	PPR	Executive summary review of recommendations Audit Committee 13 March 2013	Final DD: None	Public RD: None

11

transactions as a permanent solution. This will form part of the NetRegulate change request process. Reports are currently obtained from NetRegulate at month-end and manual adjustments are made to correct readmission charges on individual registrants' records which have been incorrectly applied and a reversing journal is posted. A project is currently underway to address the issue of NetRegulate incorrectly applying the readmission fee within the four week window where the readmission fee is not chargeable.				

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
2013-03-01	a	AUD	PPR	Executive summary review of recommendations Audit Committee 13 March 2013	Final DD: None	Public RD: None

12